ON *S*-SEMIGROUPS OF AUTOMATA

by

CORNELIS PAUL VLAGSMA.

A thesis presented for the degree of Doctor of Philosophy

at the Australian National University

Canberra,

June, 1973.

The results presented in chapters 3, 4 and 5 of this thesis are my own.

Cornelis Paul Vlagsma.

ACKNOWLEDGEMENTS.

This thesis was researched with the assistance of a Commonwealth Postgraduate Award.

I wish to thank my supervisor, Dr Martin Ward, for his encouragement during the course of the work and his suggestions during the writing of the thesis. I am also grateful to Professor Hanna Neumann, who supervised the work until her death in November 1971, and to Dr John Cossey who was my co-supervisor at the time. Thanks also to the members of the Department of Pure Mathematics, S.G.S., who provided a congenial atmosphere for study, and to Mrs A. Zalucki for being a very patient typist.

Thanks are also due to my parents, who got me this far in the first place.

And to my friends in the Union Bar who provided light relief outside working hours.

CONTENTS

INTRODUCTION

This thesis presents an investigation into the structure of *S*-semigroups of automata, a concept introduced by A.C. FLECK and S.T. HEDETNIEMI. As was pointed out by these authors in their original paper, this new means of associating a semigroup with an automaton gives rise to a semigroup which more faithfully carries the structure of the original automaton than does the classical semigroup.

The author of this thesis attempted to use the *S*-semigroups to determine series-parallel, and feedback decompositions of automata. This attempt was frustrated by a lack of knowledge of the structure of *S*-semigroups. Nor was it possible to determine the relation between an *S*-semigroup of an automaton and the *S*-semigroups of the automata involved in a decomposition of that automaton, for the same reason.

The usefulness of knowing the simple groups which divide a semigroup, in determining relationships between a product of semigroups and the factors of the product, and therefore the structure of a semigroup, was shown by KROHN and RHODES, with their prime decomposition theorem for finite semigroups.

In this thesis all the simple groups which divide the *S*-semigroup of an automaton, M, are found. It is shown that these simple groups are exactly those which divide the permutation group $P_{n(M)}$, where $n(M)$ is an invariant of the automaton M. A brief description is given of a method of finding this invariant.

It is known that the simple groups which divide a semigroup must divide a subgroup of that semigroup, and that the maximal subgroups of a semigroup are associated with the idempotents of the semigroup. Hence, in order to find the simple groups which divide a semigroup it is only necessary to find the idempotents of the semigroup, and then the simple groups which divide the groups associated with the idempotents. This is the procedure used in this thesis.

Chapter 1 is a brief introduction to the automata theory and semigroup theory required in the remainder of the paper. The second chapter contains some simple results on multiplication in semigroups which are often used in later proofs. It concludes with the definition of a class of semigroups associated with the S-semigroup of an automaton and the J classes of the semigroup of an automaton.

In chapters 3 and 4 a set of idempotents of the semigroups just mentioned is found which has the property that any simple group dividing the S-semigroup must divide one of the groups associated with the idempotents in the set.

In chapter 5 this set is reduced further and the structure of the groups associated with the idempotents is determined. It is shown that the simple groups which divide the S-semigroup of an automaton must divide a permutation group $P_{n(M)}$, where $n(M)$ is an invariant of the automaton, M. It is also shown that the permutation group $P_{n(M)}$ divides the S-semigroup. An insight into a procedure to determine the value of $n(M)$ is also given.

NOTATION

The notation introduced here is that which is not defined in the thesis.

$A \setminus B$	The complement of the set B in the set A.
$\text{Endo}_L(S)$	The collection of all endomorphisms of S considered as a subsemigroup of $F_L(S)$, the set of all mappings of S into S with multiplication defined by $f.g(s) = f(g(s))$, for all $s \in S$.
$F_R(X)$	The set of all mapping of a set X ~~S~~ into X with multiplication $f.g(s) = g(f(s))$ for all $s \in X$.
LCM	Lowest common multiple.
S^1	The semigroup S if S is a monoid, otherwise $S^1 = S \cup \{1\}$, where $1 \notin S$, multiplication in S is unchanged an 1 acts as an identity for $S \cup \{1\}$.
$\emptyset$	The empty set.
Z^+	The positive integers
P_n	The permutation group on n characters.

CHAPTER 1. DEFINITIONS AND PRELIMINARIES

1.1 REMARK. We define the concepts of automaton, semigroup of an automaton, and *S*-semigroup of an automaton. This is followed by some general semigroup theory including the introduction of the Green relations on semigroups and the concepts of division of semigroups and the semidirect product of semigroups. The chapter concludes with a discussion of a method to find all the simple groups which divide a given semigroup.

1.2 DEFINITION FINITE AUTOMATON

An automaton M is a triple (Q,I,λ), where Q is a finite set called the state set of M, I is a finite set called the input alphabet of M and $\lambda : Q \times I \to Q$ is a mapping called the next state function.

We shall assume that all automata with which we deal are of this kind.

1.3 DEFINITION SEMIGROUP of an AUTOMATON

Let I^* be the free monoid on the input alphabet I of an automaton $M = (Q,I,\lambda)$.

Define a mapping $\lambda^* : Q \times I^* \to Q$ as follows :

$\lambda^*(q,\Lambda) = q$, for all $q \in Q$, where Λ is the empty string in I^*

and $\lambda^*[q,(x_1,\ldots,x_n)] = \lambda^*[\lambda(q,x_1),(x_2,\ldots,x_n)]$ for all strings $(x_1,\ldots,x_n)$ in I^*, and for all $q \in Q$.

Define the map $\psi : I^* \to F_R(Q)$ as follows :

$$\psi : (x_1,\ldots,x_n) \mapsto t \text{ where } t : q \mapsto \lambda^*(q,(x_1,\ldots,x_n)) \text{ for all}$$

$q \in Q$, whenever $(x_1,\ldots,x_n) \in I^*$.

This mapping will be an homomorphism and we call $\psi(I^*)$, the image of I^* in $F_R(Q)$ under ψ, the SEMIGROUP of the AUTOMATON and denote it $S(M)$.

Certainly $S(M)$ is finite whenever the automaton is.

When $q,q' \in Q$ and $s \in S(M)$ we shall write $q \circ s = q'$ iff $\lambda^*(q,x) = q'$ where $x \in I^*$ and $\psi(x) = s$. We see that $q.s$ denotes the action of the transformation s of $F_R(Q)$ on the element q of Q.

1.4 DEFINITION S-SEMIGROUP of an AUTOMATON [FLECK & HEDETNIEMI].

Let $M = (Q,I,\lambda)$ be an automaton. We shall call a triple $(q,s,q') \in Q \times S(M) \times Q$ a triple of the automaton whenever $q.s = q'$. We denote by $T(M)$ the set of all triples of the automaton M.

Define a partial product of triples as follows :

Let $(q,s,q'), (p,t,p') \in T(M)$.

Then $(q,s,q')\,(p,t,p') = (q,st,p')$ whenever $q' = p$, and is undefined otherwise.

Suppose T_1,T_2 are subsets of $T(M)$. Define the product of T_1 and T_2 by :

$$T_1T_2 = \{(q,s,q')(p,t,p') \mid (q,s,q') \in T_1,\ (p,t,p') \in T_2$$
$$\text{and their product is defined}\}.$$

If none of the products of triples of T_1 and T_2 is defined then their product is the empty set.

The multiplication is easily shown to be associative.

We define the S-SEMIGROUP of the AUTOMATON, denoted $S(M)$, to be the power semigroup on the set $T(M)$ with multiplication as defined above.

That is, $S(M)$ is the collection of all subsets of $T(M)$, with the given multiplication. Certainly $S(M)$ is finite whenever M is finite.

1.5 REMARK Since each element of the S-semigroup $S(M)$ of an automaton M is a subset of the set $T(M)$ of triples of the automaton we may use the properties of set inclusion, union and intersection between the elemtns of $S(M)$.

Further it can be seen that the set $T(M)$ is naturally embedded in $S(M)$ under the mapping $\phi : T(M) \rightarrow S(M)$ defined by $\phi : (q,s,q') \mapsto \{(q,s,q')\}$, with the product of singletons in $S(M)$ being the empty set whenever the product of their preimages under ϕ is undefined. Following the usual practice in algebra we shall identify the elements (q,s,q') of $T(M)$ with the elements $\{(q,s,q')\}$ of $S(M)$ and treat them accordingly.

1.6 REMARK The remainder of the chapter will deal with definitions and results from the theory of semigroups in general. Most of the results are in ARBIB while the balance may be found in CLIFFORD & PRESTON.

1.7 DEFINITION DUALITY

The DUAL $d(A)$ of a proposition or concept, A, is that proposition or concept which is produced by replacing every semigroup product xy by the reverse product yx in the original proposition or concept, A.

It is true that if A and B are propositions and A implies B, then d(A) implies d(B). Thus if a theorem is true then so is its dual. We shall make consistent use of this fact.

Whenever a concept and its dual are introduced we shall note this. Some concepts are self dual. Notice that $d(d(A)) = A$.

1.8 DEFINITION The GREEN RELATION on a SEMIGROUP [GREEN].

Let S be a semigroup. For $s \in S$ we write $L(s) = S^1 s$, $R(s) = sS^1$ and $J(s) = S^1 s S^1$. We define the following binary relations $\mathcal{J}, \mathcal{R}, \mathcal{L}, \mathcal{H}$ on S.

(i) $s_1 \mathcal{J} s_2$ iff $J(s_1) = J(s_2)$

(ii) $s_1 \mathcal{L} s_2$ iff $L(s_1) = L(s_2)$

(iii) $s_1 \mathcal{R} s_2$ iff $R(s_1) = R(s_2)$

(iv) $s_1 \mathcal{H} s_2$ iff $s_1 \mathcal{L} s_2$ and $s_1 \mathcal{R} s_2$

Notice that the concepts of $\mathcal{L}$ relation and $\mathcal{R}$ relation are dual, and that the concepts of $\mathcal{J}$ relation and $\mathcal{H}$ relation are each self-dual.

1.9 FACT (i) $\mathcal{L}, \mathcal{R}, \mathcal{J}, \mathcal{H}$ are equivalence relations on s. We denote L_s, R_s, J_s and H_s the $\mathcal{L}, \mathcal{R}, \mathcal{J}, \mathcal{H}$ equivalence classes, respectively, containing the element s of S.

(ii) $s_1 \mathcal{J} s_2$ iff there exist $w,x,y,z \in S^1$ such that $xs_1y = s_2$ and $zs_2w = s_1$.

(iii) $s_1 \mathcal{R} s_2$ iff there exist $x,y \in S^1$ such that $s_1x = s_2$ and $s_2y = s_1$.

(iv) $s_1 \mathcal{L} s_2$ iff there exist $x,y \in S^1$ such that $xs_1 = s_2$ and $ys_2 = s_1$.

1.10 DEFINITION Let S be a semigroup. We define the following orderings on the $\mathcal{J},\mathcal{L},\mathcal{R}$ classes of S.

(i) $J_{s_1} \leq J_{s_2}$ iff $J(s_1) \subseteq J(s_2)$

(ii) $L_{s_1} \leq L_{s_2}$ iff $L(s_1) \subseteq L(s_2)$

(iii) $R_{s_1} \leq R_{s_2}$ iff $R(s_1) \subseteq R(s_2)$

1.11 FACT Let S be a finite semigroup. Then the following are true :

(i) $\mathcal{J}$ classes are disjoint unions of $\mathcal{R}$ classes.

(ii) $\mathcal{J}$ classes are disjoint unions of $\mathcal{L}$ classes.

(iii) Within a $\mathcal{J}$ class the intersection of any $\mathcal{L}$ and any $\mathcal{R}$ class is nonempty and is an $\mathcal{H}$ class.

(iv) Each $\mathcal{L}$ class of a $\mathcal{J}$ class contains an idempotent.

(v) Each $\mathcal{R}$ class of a $\mathcal{J}$ class contains an idempotent.

1.12 FACT Let S be a finite semigroup. Let $s_1,s_2 \in S$ with $s_1 \mathcal{J} s_2$. Let $x,y \in S^1$ with $xs_1y = s_2$. Then the map $\alpha : H_{s_1} \to H_{s_2}$, defined by $\alpha : t \mapsto xty$ for all $t \in H$, is both 1:1 and onto.

From this it can be seen that any two $\mathcal{H}$ classes contained in the same $\mathcal{J}$ class of S must be in 1:1 correspondence.

1.13 FACT The maximal subgroups of a semigroup S are exactly those $\mathcal{H}$ classes of S which contain idempotents.

1.14 DEFINITION DIVISION of SEMIGROUPS.

Let S_1,S_2 be semigroups. We say S_1 divides S_2, written $S_1|S_2$ iff there exists an homomorphism from a subsemigroup of S_2 onto S_1.

1.15 LEMMA (i) The division of semigroups is transitive.

(ii) Let $\phi : S_1 \to S_2$ be a 1:1 homomorphism. Then $S_1|S_2$.

Proof: (i) obvious.

(ii) $\phi(S_1)$ is a subsemigroup of S_2 isomorphic to S_1, and $\phi^{-1} : \phi(s_1) \to S_1$ is an epimorphism. #

This fact will be used extensively in future proofs.

1.16 DEFINITION SEMIDIRECT PRODUCT of SEMIGROUPS.

Let S_1 and S_2 be semigroups and let $\phi : S_1 \to \text{Endo}_L(S_2)$ be an homomorphism. Then the set $S_2 \times S_1$ with multiplication defined by :

$$(s_2,s_1).(s_2',s_1') = (s_2[\phi(s_1)(s_2')],s_1s_1')$$

is called the semidirect product of S_2 by S_1 with connecting homomorphism ϕ.

We denote the product by $S_2 \times_\phi S_1$.

1.17 DEFINITION IRREDUCIBLE SEMIGROUPS.

A semigroup S is irreducible if, whenever $S|S_1wS_2$, (where S_1 and S_2 are semigroups and S_1wS_2 is their wreath product as defined in ARBIB) then $S|S_1$ or $S|S_2$.

From ARBIB we know that if S is irreducible and $S|S_2 \times_\phi S_1$ or $S|S_1 \times S_2$ (the direct product), then $S|S_1$ or $S|S_2$.

1.18 FACT Simple groups are irreducible.

<u>1.19 FACT</u> Let G be a group and let S be a semigroup such that $G|S$. Then there exists a subgroup G' of S such that $G|G'$.

<u>1.20 REMARK</u> Our problem is to find the simple groups which may divide the $\mathcal{S}$-semigroup $\mathcal{S}(M)$ of an automaton M.

In order to do this we need only determine the maximal subgroups of $\mathcal{S}(M)$ (1.19). This can be achieved by finding the structures of those $\mathcal{H}$ classes of $\mathcal{S}(M)$ which contain idempotents (1.13).

It will be found that in determining the structure of the $\mathcal{H}$ classes we show them to be groups dividing the direct or semidirect products of groups whose structure we know. Facts 1.18 and 1.13(i) show that the simple groups dividing $\mathcal{S}(M)$ must divide the groups involved as factors of these products.

CHAPTER 2. PROPERTIES of the SEMIGROUPS of AUTOMATA

2.1 REMARK In this chapter we introduce some notation for properties of the elements of the semigroup of an automaton, and demonstrate some properties of multiplication in the semigroup. The chapter concludes with the definition of certain semigroups associated with the S-semigroup of an automaton, which will be used extensively in later chapters.

2.2 DEFINITION Let $M = (Q,I,\lambda)$ be an automaton with semigroup $S(M)$.

Let $s \in S(M)$. Then we may consider s as an element of $F_R(Q)$, i.e. s is a mapping $s : Q \to Q$.

(i) Define the equivalence relation, $P(s)$, induced on Q by s as follows :

$$P(s) = \{(p,q) \in Q \times Q \mid p.s = q.s\}$$

(ii) Define the final state set, $Z(s)$, of s, by :

$$Z(s) = \{q \in Q \mid \exists p \in Q \text{ and } p.s = q\}$$

(iii) Given $s,t \in S(M)$ we shall say that t covers s, denoted $Z(s)|P(t)$, iff $|Z(s)| = \#P(t)$ and for all $p,q \in Z(s)$ such that $p \neq q$ we have $(p,q) \notin P(t)$.

Here $|Z(s)|$ denotes the cardinality of $Z(s)$, and $\#P(t)$ is the number of blocks in the partition induced on Q by the equivalence relation $P(s)$. That is

$$\#P(t) = \max_{R \in T_p} |R|, \text{ where } T_p = \{(p_1,\ldots,p_n) \subseteq Q \mid (p_i,p_j) \in P(t) \text{ iff } i = j\}$$

We use the partial ordering, induced by set inclusion, on the equivalence relations on a set, and notice that if P and R are equivalence relations on Q then $P \leq R \Rightarrow \#P \geq \#R$.

Obviously if $s \in S(M)$ then $\#P(s) = |Z(s)|$.

<u>2.3 LEMMA</u> Let $x,y \in S(M)$.

Then (i) $P(xy) \geq P(x)$, $\#P(xy) \leq \#P(x)$

(ii) $Z(xy) \subseteq Z(y)$, $|Z(xy)| \leq |Z(y)|$

(iii) $\#P(xy) \leq \#P(y)$

(iv) $|Z(xy)| \leq |Z(x)|$

<u>Proof</u> : (i) Let $(p,q) \in P(y)$. Then $p.x = q.x$, and $(p.x) = (q.x).y$. Thus $p.xy = q.xy$ and $(p,q) \in P(xy)$. Hence $P(x) \leq P(xy)$.

(ii) Let $q \in Z(xy)$. Then there exists $p \in Q$ such that $p.xy = q$. Thus $(p.x).y = q$, and since $p.x \in Q$ we must have $q \in Z(y)$. Hence $Z(xy) \subseteq Z(y)$.

(iii) $\#P(x) \geq \#P(xy)$ implies $|Z(x)| \geq |Z(xy)|$.

(iv) $|Z(y)| \geq |Z(xy)|$ implies $\#P(y) \geq \#P(xy)$. #

<u>2.4 LEMMA</u> Let $x \mathcal{J} y$ in $S(M)$.

Then $|Z(x)| = |Z(y)|$, and $\#P(x) = \#P(y)$.

<u>Proof</u> :

$x \mathcal{J} y$ implies the existence of $r,s,t,v \in S(M)$ such that $rxs = y$ and $tyv = x$. Now $|Z(x)| \geq |Z(rx)| \geq |Z(rxs)| = |Z(y)|$. Similarly $|Z(y)| \geq |Z(ty)| \geq |Z(tyv)| = |Z(x)|$. Thus $|Z(x)| = |Z(y)|$. That $\#P(x) = \#P(y)$ follows immediately. #

2.5 LEMMA $Z(x)|P(y) \Leftrightarrow |Z(xy)| = |Z(x)| = |Z(y)|$.

Proof : $Z(x)|P(y)$ implies $|Z(x)| = \#P(y) = |Z(y)|$.

Let $p,q \in Z(x)$ such that $p \neq q$. Then $(p,q) \notin P(y)$ and $p.y \neq q.y$. Further $p.y, q.y \in Z(xy)$. Thus $|Z(xy)| \geq |Z(x)|$. But $|Z(x)| \geq |Z(xy)|$, so that $|Z(x)| = |Z(xy)| = |Z(y)|$.

Conversely when $|Z(xy)| = |Z(y)|$ we must have $Z(xy) = Z(y)$. Suppose $Z(x) = \{p_1,\dots,p_n\}$. Then $\{p_1.y,\dots,p_n.y\} \subseteq Z(xy)$. Further $q \in Z(xy)$ implies that $q = p.xy$ for some $p \in Q$. But $p.x = p_i$ for some $1 \leq i \leq n$, so that $q = p_i.y$ for some $p_i \in Z(x)$. Thus $\{p_1.y,\dots,p_n.y\} \supseteq Z(xy)$, and $Z(y) = Z(xy) = \{p_1.y,\dots,p_n.y\}$. Also $p_iy = p_jy$ iff $p_i = p_j$, so that $(p_i,p_j) \in P(y)$ iff $p_i = p_j$. Thus $Z(x)|P(y)$. #

2.6 LEMMA Let $x^2 = x \in S(M)$. Then for all $q \in Z(x)$, $q.x = q$.

Proof : $x^2 = x$ implies $|Z(x)| = |Z(x^2)|$, so that $Z(x)|P(x)$.

Let $q \in Z(x)$. Then there exists $p \in Q$ such that $p.x = q$. But $q = p.x = p.x^2 = (p.x).x = q.x$. #

2.7 LEMMA Let $x,y \in S(M)$.

Then (i) $y\,\mathcal{R}\,x \Leftrightarrow P(x) = P(y)$

(ii) $y\,\mathcal{L}\,x \Leftrightarrow Z(x) = Z(y)$.

Proof :(i) $y\,\mathcal{R}\,x$ implies the existence of $r,s \in S(M)$ such that $yr = x$, $xs = y$. Thus $P(y) \leq P(x)$ and $P(x) \leq P(y)$ so that $P(x) = P(y)$. Conversely suppose $P(x) = P(y)$. There exist $w^2 = w$ and $v^2 = v$ such that $w\,\mathcal{R}\,x$ and $v\,\mathcal{R}\,y$ [1.11 (iv) & (v)]. Thus $P(w) = P(x) = P(y) = P(v)$. Also $Z(w)|P(w) = P(v)$ and

$Z(v)|P(v) = P(w)$. Let $p \in Q$, and $p.v = q$. There exists $r \in Z(w)$ such that $(r,p) \in P(v)$. But $r.w = r$, so that $r.wv = (r.w).v = r.v = p.v = q$. Now $(r,p) \in P(w) = P(v)$, so that $p.wv = q$. Thus $wv = v$. Similarly it may be shown that $vw = w$. Hence $w \mathcal{R} v$, and $x \mathcal{R} w \mathcal{R} v \mathcal{R} y$, so that $x \mathcal{R} y$.

(ii) $y \mathcal{L} x$ implies the existence of $r,s \in S(M)$ such that $ry = x$ and $sx = y$. Thus $Z(x) \subseteq Z(y)$ and $Z(y) \subseteq Z(x)$, so that $Z(y) = Z(x)$. Conversely let $Z(x) = Z(y)$. Then there exist $w^2 = w$ and $v^2 = v$ in $S(M)$ such that $w \mathcal{L} x$ and $v \mathcal{L} y$. Thus $Z(x) = Z(w) = Z(v) = Z(y)$. We have $Z(v) = Z(w)|P(w)$ and $Z(w) = Z(v)|P(v)$. Suppose $p \in Q$ and $p.v = q$. Then $q \in Z(v) = Z(w)$ implies $q.w = q$, and $p.vw = q$. Thus $v = vw$. Similarly $w = wv$. Thus $w \mathcal{L} v$ and $x \mathcal{L} w \mathcal{L} v \mathcal{L} y$. Hence $x \mathcal{L} y$. #

<u>2.8 LEMMA</u> Let $x \mathcal{J} y$ in $S(M)$.

Then $Z(x)|P(y) \Leftrightarrow xy \mathcal{R} x \Leftrightarrow xy \mathcal{L} y \Leftrightarrow xy \mathcal{J} x$.

<u>Proof</u> : $Z(x)|P(y)$ implies $\#P(x) = \#P(y) = \#P(xy)$. Since $P(xy) \leq P(x)$ we have $P(xy) = P(x)$. Thus $xy \mathcal{R} x$.

Also $|Z(x)| = |Z(y)| = |Z(xy)|$ and $Z(xy) \subseteq Z(y)$. Thus $Z(xy) = Z(y)$ and $xy \mathcal{L} y$.

Certainly $xy \mathcal{J} x$ and $xy \mathcal{J} y$.

Conversely we have that $xy \mathcal{J} x$ and $x \mathcal{J} y$ imply $|Z(xy)| = |Z(x)| = |Z(y)|$. Thus $Z(x)|P(y)$. The cases $xy \mathcal{R} x$ and $xy \mathcal{L} y$ are special cases of this.

2.9 LEMMA (i) Let $y \mathcal{R} x$, $z \mathcal{J} x$ in $S(M)$ with $yz \mathcal{J} x$. Then $yz \mathcal{R} x$.

(ii) Let $y \mathcal{J} x$, $z \mathcal{L} x$ in $S(M)$ with $yz \mathcal{J} x$. Then $yz \mathcal{L} x$.

(iii) Let $y \mathcal{R} x$, $z \mathcal{L} x$ in $S(M)$ with $yz \mathcal{J} x$. Then $yz \mathcal{H} x$.

Proof : (i) $yz \mathcal{J} x$ and $x \mathcal{J} y \mathcal{J} z$ imply $|Z(yz)| = |Z(x)| = |Z(y)| = |Z(z)|$.

Thus $Z(y)|P(z)$. Thus $yz \mathcal{R} y \mathcal{R} x$, i.e. $yz \mathcal{R} x$.

Parts (ii) and (iii) are similar.

2.10 LEMMA Let $x^2 = x \in S(M)$.

Then (i) $y \mathcal{R} x \Rightarrow xy = y$

(ii) $y \mathcal{L} x \Rightarrow yx = y$.

Proof : (i) $y \mathcal{R} x$ implies $P(y) = P(x)$. Let $p \in Q$, and $p.y = q$. Then there exists $r \in Z(x)$ such that $(p,r) \in P(y)$ and $r.y = q$. Now $r.x = r$ so that $r.xy = q$. Also $Z(x)|P(x) = P(y)$, and $xy \mathcal{R} x$. Thus $(p,r) \in P(xy) = P(x)$, and $p.xy = q$. Thus $xy = y$.

(ii) $y \mathcal{L} x$ implies $Z(y) = Z(x)$. Let $p \in Q$ and $p.y = q$. Then $q \in Z(y)$ and $q.x = q$. Thus $p.yx = q$. Hence $yx = y$. #

2.11 REMARK The results proven above will be extensively used through this paper and will generally be applied without comment.

We now define a set of semigroups associated with the S-semigroup of an automaton, which will play a major part in the development of this thesis. We also prove a result on idempotents in these semigroups.

2.12 DEFINITION We have seen in the first chapter that the S-semigroup, $S(M)$, of an automaton, M, is the collection of all subsets of the set of triples $T(M)$.

Suppose $\{J_1,\ldots,J_n\}$ is a set of J classes of $S(M)$, such that whenever $J_i \leq J \leq J_k$ for $1 \leq i,k \leq n$, then $J \in \{J_1,\ldots,J_n\}$. We say ~~We define :~~ that $\{J_1,\ldots,J_n\}$ is J-closed.

Define $S(\bigcup_{i=1}^{n} J_i) = \{s \in S(M) | x \in \bigcup_{i=1}^{n} J_i$ for all $(p,x,q) \in s\}$,

with multiplication defined by :

$$s.t = \{(p,x,q) \in st | x \in \bigcup_{i=1}^{n} J_i\} \text{ where } s,t \in S(\bigcup_{i=1}^{n} J_i)$$

and st is the product of s and t in $S(M)$.

It is easily seen that $S(\bigcup_{i=1}^{n} J_i)$ is a semigroup.

Notice also that if $\{J_1',\ldots,J_m'\} \subseteq \{J_1,\ldots,J_n\}$, and is J-closed, then any element of $S(\bigcup_{i=1}^{m} J_i')$ may be considered as an element of $S(\bigcup_{i=1}^{n} J_i)$. Further the semigroup $S(\bigcup_{i=1}^{m} J_i')$ divides $S(\bigcup_{i=1}^{n} J_i)$. ~~However the former is not necessarily a subsemigroup of the latter.~~ Obviously $S(M) = S(S)$, since S is the union of all its J classes.

We shall use the dot in the multiplication $s.t$ of elements of $S(\bigcup_{i=1}^{n} J_i)$ to represent multiplication of the elements in that semigroup. Since we sometimes deal with more than one semigroup of this type the product may be ambiguous. In these cases the semigroup wherein the multiplication occurs will be specified. Whenever we use $S(\bigcup_{i=1}^{n} J_i)$ we shall assume that $\{J_1,\ldots,J_n\}$ is J-closed. Obviously $\{J\}$ is J-closed, so that $S(J)$ is a semigroup.

<u>2.13 DEFINITION</u> Let $t \in S(\bigcup_{i=1}^{n} J_i)$.

Define $N(t) = \{(q,x,q) \in t \mid x^2 = x \in S(M)\}$.

<u>2.14 LEMMA</u> Let $s.s = s \in S(J)$ where J is a $\mathcal{J}$ class of $S(M)$, i.e. s is an idempotent in $S(J)$.

Then $s = s.N(s).s$

<u>Proof</u> : Put $k = |s|$, considering s as a subset of $T(M)$.

Let $(p,x,q) \in s$.

Then $(p,x,q) \in s^{k+1} = s$.

i.e. $(p,x,q) = \prod_{i=1}^{k+1} (p_i,x_i,p_{i+1})$ where $(p_i,x_i,p_{i+1}) \in s$ for $1 \leq i \leq k+1$.

But $k = |S|$, thus there exist integers ℓ,m such that $1 \leq \ell < m \leq k+1$, and $(p_\ell,x_\ell,p_{\ell+1}) = (p_m,x_m,p_{m+1})$.

Suppose $x_{m-1}x_m \in J_1$. Then $J = J_{x_m} \geq J_1$. But $(\prod_{i=1}^{m-2} x_i)x_{m-1}x_m(\prod_{i=m+1}^{k+1} x_i) = x$, so $J_1 \geq J$.

Thus $J_1 = J$, and $x_{m-1}x_m \in J$.

Hence $Z(x_{m-1}) \mid P(x_m) = P(x_\ell)$.

Put $y = \prod_{i=\ell}^{m-1} x_i$. Now $y \,\mathcal{J}\, x_i$, $1 \leq i \leq k+1$, thus $y \,\mathcal{R}\, x_\ell$ and $y \,\mathcal{L}\, x_{m-1}$.

Thus $Z(y) \mid P(y)$, so that $y^r \,\mathcal{H}\, y$ for all $r \in Z^+$. Now there exists $t \in Z^+$ such that $y^t = y^{2t}$. Thus H_{y^t} is a subgroup of $S(M)$, and $y^t y = y$.

Now $(p_\ell,y,p_m) \in s$ so that $(p_\ell,y^t,p_\ell) \in s$.

But $(p_\ell, y^t, p_\ell) \in N(s)$.

$$\text{Thus } (p,y,q) = \prod_{i=1}^{\ell-1} (p_i,x_i,p_{i+1}).(p_\ell,y,p_m).\prod_{i=m}^{k+1} (p_i,x_i,p_{i+1})$$

$$= \prod_{i=1}^{\ell-1} (p_i,x_i,p_{i+1}).(p_\ell,y^t,p_2).(p_\ell,y,p_m).\prod_{i=m}^{k+1} (p_i,x_i,p_{i+1})$$

$$\varepsilon\ s.N(s).s.$$

Thus $s \leq s.N(s).s \leq s^3 = s$.

Therefore $s = s.N(s).s$. #

CHAPTER 3. THE SUBGROUPS of $S(M)$.

3.1 INTRODUCTION In this chapter we shall demonstrate that the subgroup which is the H class associated with an idempotent of an S-semigroup, $S(M)$, divides a direct product of subgroups associated with idempotents of the semigroups $S(J)$ where each J is a J class of the semigroup $S(M)$.

Suppose s is an idempotent in $S(M)$. Let $\{J_1,\ldots,J_m\}$ be ~~the~~ a J-closed set of J classes of $S(M)$ such that for all $(p,x,q) \varepsilon s$, $x \varepsilon J_i$ for some $1 \leq i \leq m$. ~~and for each J_i there exists $(p,x,q) \varepsilon s$ such that $x \varepsilon J_i$.~~ Then we may consider s as an element of $S(\bigcup_{i=1}^{m} J_i)$. We show that there exist subsets of s which are idempotents when considered as elements of the semigroups $S(J_i)$. Each element of the group H_s is found to contain subsets which are elements of the groups associated with the idempotents in the $S(J_i)$. The group elements are in fact uniquely determined by these subsets and s. Using these facts it is shown that the group H_s divides the direct product of the groups which are the H classes of the idempotents in the semigroups $S(J_i)$ for $1 \leq i \leq m$.

3.2 DEFINITION Let $\{J_1,\ldots,J_m\}$ be a J-closed set of J classes of $S(M)$ such that $s \varepsilon S(\bigcup_{i=1}^{m} J_i)$ and $s^2 = s \varepsilon S(M)$. Then $s.s = s \varepsilon S(\bigcup_{i=1}^{m} J_i)$.

(i) Define $s_i = \{(p,x,q) \varepsilon s | x \varepsilon J_i\}$ for $1 \leq i \leq m$.

(ii) Define $E(s_i)$ as follows for $1 \leq i \leq m$; $E(s_i) \subseteq s_i$ such that $E(s_i).E(s_i) = E(s_i)$ (multiplication in $S(J_i)$), and if there exists s_i' such that $E(s_i) \subseteq s_i' \subseteq s_i$ and $s_i'.s_i' = s_i'$, then $s_i' = E(s_i)$.

That is, $E(s_i)$ is maximal in s_i with respect to the property of idempotence in $S(J_i)$.

We shall show that $E(s_i)$ is unique in each s_i.

<u>3.3 LEMMA</u> Let $s.s = s \in S(\bigcup_{i=1}^{m} J_i)$. Let $\{E(s_i) | 1 \le i \le m\}$ have the property defined above.

Then $s_i.E(s_i) \subseteq E(s_i)$ and $E(s_i).s_i \subseteq E(s_i)$ in $S(J_i)$ for $1 \le i \le m$.

<u>Proof</u> : We have $[E(s_i) \cup s_i.E(s_i)]^2 \supseteq E(s_i)^2 \cup s_i.E(s_i)^2 = E(s_i) \cup s_i.E(s_i)$.

Now $E(s_i) \cup s_i.E(s_i)$ is an element of the finite semigroup $S(J_i)$, so there exists $n \in Z^+$ such that $[E(s_i) \cup s_i.E(s_i)]^n$ is an idempotent in $S(J_i)$.

Since $s.s = s$ in $S(\bigcup_{i=1}^{m} J_i)$ we must have $s_i.s_i \subseteq s_i$ in $S(J_i)$. Certainly $E(s_i) \cup s_i.E(s_i) \subseteq s_i$ and thus

$$s_i \supseteq [E(s_i) \cup s_i.E(s_i)]^n \supseteq E(s_i) \cup s_i.E(s_i) \supseteq E(s_i) .$$

By the definition of $E(s_i)$, it is maximal with respect to idempotence, so we have

$$E(s_i) = [E(s_i) \cup s_i.E(s_i)]^n \supseteq E(s_i) \cup s_i.E(s_i) .$$

Thus $s_i.E(s_i) \subseteq E(s_i)$.

$E(s_i).s_i \subseteq E(s_i)$ is the dual of the first part.

All multiplication in the proof occurs within $S(J_i)$ except where otherwise stated. #

<u>3.4 COROLLARY</u> The $E(s_i)$ defined in 3.2 are unique, for $1 \leq i \leq m$.

<u>Proof</u> : Suppose $E(s_i)$ and $E'(s_i)$ have the property of maximality of idempotence in s_i, for $1 \leq i \leq m$.

Then

$$[E(s_i) \cup E'(s_i)]^2 = E(s_i)^2 \cup E'(s_i)^2 \cup E(s_i).E'(s_i) \cup E'(s_i).E(s_i)$$

$$\subseteq E(s_i) \cup E'(s_i) \cup E(s_i) \cup E'(s_i)$$

$$= E(s_i) \cup E'(s_i)$$

$$\subseteq [E(s_i) \cup E'(s_i)]^2 .$$

Thus $[E(s_i) \cup E'(s_i)]^2 = E(s_i) \cup E'(s_i)$ and the result follows from the definition.

<u>3.5 REMARK</u> Having defined these idempotents in the $S(J_i)$ for any $s.s = s \in S(\bigcup_{i=1}^{m} J_i)$ we shall now show that each group element of H_s contains a subset which is a group element of $H_{E(s_i)}$, for $1 \leq i \leq m$, whenever $E(s_i) \neq \phi$.

<u>3.6 DEFINITION</u> Let $t \in S(\bigcup_{i=1}^{m} J_i)$.

Define $t_i = \{(p,x,q) \in t | x \in J_i\}$ for $1 \leq i \leq m$.

<u>3.7 LEMMA</u> Let $s.s = s \in S(\bigcup_{i=1}^{m} J_i)$, and $(q_1,y_1,q_1) \in N(E(s_i))$.

Let $g \in H_s$ such that $g^n = s$.

Let $\{(q_1,x_1,q_2),\ldots,(q_n,x_n,q_1)\} \subseteq g$ such that $\prod_{i=1}^{n} x_i = y_1$.

Put $y_k = (\prod_{i=k}^{n} x_i).y_1.(\prod_{i=1}^{k-1} x_i)$ for $2 \leq k \leq n$.

Then $y_k^2 = y_k$ and $y_k \mathcal{J} y_1$ for $1 \leq k \leq n$.

<u>Proof</u> : Certainly a subset $\{(q_1,x_1,q_2),\ldots,(q_n,x_n,q_1)\}$ of g exists, otherwise $(q_1,y_1,q_1) \notin g^n = s$.

Put $r_k = \prod_{i=k}^{n} x_i$ for $1 \leq k \leq n$, $t_k = \prod_{i=1}^{k-1} x_i$ for $2 \leq k \leq n$, and $t_1 = y_1$.

Notice that $t_k r_k = y_1$ for $1 \leq k \leq n$.

Now $y_k = r_k y_1 t_k$. Thus $y_k^2 = r_k y_1 t_k r_k y_1 t_k = r_k y_1^3 t_k = r_k y_1 t_k = y_k$ for $1 \leq k \leq n$.

Also $y_k = r_k y_1 t_k$ implies $J_{y_1} \geq J_{y_k}$.

But $y_1 = y_1^3 = t_k r_k y_1 t_k r_k = t_k y_k r_k$ so that $J_{y_k} \geq J_{y_1}$.

Thus $y_k \mathcal{J} y_1$ for $1 \leq k \leq n$. #

<u>3.8 REMARK</u> We notice that

$$s = g^{n-k+1}.s.g^{k-1} \ni \prod_{i=1}^{n} (q_i,x_i,q_{i+1}).(q_1,y_1,q_1).\prod_{i=1}^{k-1} (q_i,x_i,q_{i+1}) = (q_k,y_k,q_k)$$

where $q_{n+1} = q_1$, for $2 \leq k \leq n$.

Further $(q_k,y_k,q_k) \in s_i$, and since $y_k^2 = y_k$ we must have $(q_k,y_k,q_k) \in N[E(s_i)]$.

<u>3.9 LEMMA</u> Given the conditions of the previous lemma, put $x_k' = y_k x_k$ for $1 \leq k \leq n$, and put $r_k' = (\prod_{i=k}^{n} x_i')y_1$ for $1 \leq k \leq n$; $t_k' = \prod_{i=1}^{k-1} x_i'$ for $2 \leq k \leq n$; $t_1' = y_1$.

Then $y_k = r_k' t_k'$ and $x_k' \mathcal{J} y_1$, for $1 \leq k \leq n$.

<u>Proof</u> : Notice first that $y_1 t_k = y_1^3 t_k = y_1 t_k r_k y_1 t_k = y_1 t_k y_k$, and $r_k y_1 = r_k y_1^3 = r_k y_1 t_k r_k y_1 = y_k r_k y_1$ for $1 \leq k \leq n$.

Now $t_1' = y_1 = y_1^2 = y_1 t_1$.

Suppose $t_i' = y_1 t_i$ for $1 \leq i \leq n - 1$.

Then $t_{i+1}' = t_i' y_i x_i = y_1 t_i y_i x_i = y_1 t_i x_i = y_1 t_{i+1}$.

Thus $t_k' = y_1 t_k$ for $1 \leq k \leq n$.

Similarly $r_n' = y_n x_n y_1 = y_n r_n y_1 = r_n y_1$.

Suppose $r_i' = r_i y_1$ for $2 \leq i \leq n$.

Then $r_{i-1}' = x_{i-1}' r_i' = y_{i-1} x_{i-1} r_i y_1 = y_{i-1} r_{i-1} y_1 = r_{i-1} y_1$.

Thus $r_k' = r_k y_1$ for $1 \leq k \leq n$.

Now $y_k = r_k y_1 t_k = r_k y_1^2 t_k = r_k' t_k'$ for $1 \leq k \leq n$.

Also $x_k' = y_k x_k$ so that $J_{y_k} \geq J_{x_k'}$. But

$y_1 = y_1^3 = y_1 t_k r_k y_1 = t_k' r_k'$.

Thus $y_1 = t_k' x_k' r_{k+1}'$ for $1 \leq k \leq n - 1$, and $y_1 = t_n' x_n'$,

so that $J_{x_k'} \geq J_{y_1}$ for $1 \leq k \leq n$. Now $J_{y_1} = J_{y_k}$.

Hence $x_k' \, J \, y_1$ for $1 \leq k \leq n$. #

<u>3.10 REMARK</u> Let $\{x_1', x_2', \ldots, x_n'\}$ be as defined in the previous lemma. Put $x_n'' = x_n' y_1$. Then $y_k x_k' = x_k'$ for $1 \leq k \leq n - 1$, and $y_k x_n'' = x_n''$. Further we have $y_k = r_k' t_{k-1} x_{k-1}'$ for $2 \leq k \leq n$, and $y_1 = r_1' t_1' = (\prod_{i=1}^{n-1} x_i').x_n''$. Thus $y_k \, L \, x_{k-1}'$ for $2 \leq k \leq n$ and $y_1 \, L \, x_n''$, so that $x_{k-1}' y_k = x_{k-1}'$ for $2 \leq k \leq n$ and $x_n'' y_1 = x_n''$.

From this we see that

$(q_k, x_k', q_{k+1}) = (q_k, y_k, q_k).(q_k, x_k, q_{k+1}).(q_{k+1}, y_{k+1}, q_{k+1})$ for $1 \leq k \leq n-1$,

and $(q_n, x_n'', q_1) = (q_n, y_n, q_n).(q_n, x_n, q_1).(q_1, y_1, q_1)$.

Thus

$\{(q_1,x_1',q_2),\ldots,(q_{n-1},x_{n-1}',q_n),(q_n,x_n'',q_1)\} \subseteq N[E(s_i)].g.N(E(s_i)]$,

when $y_1 \in J_i$, and the multiplication is in $S(\bigcup_{i=1}^{m} J_i)$. The subset is also a subset of g_i.

Hence, for any element of $N[E(s_i)]$ such a subset exists, thus $N[E(s_i)] \subseteq \{N[E(s_i)].g.N[E(s_i)]\}_i^n$, for any element g of H_s, where H_s is the H class of s in $S(\bigcup_{i=1}^{m} J_i)$.

<u>3.11 DEFINITION</u> Let $s.s = s \in S(\bigcup_{i=1}^{m} J_i)$, and let $g \in H_s$.

Define $E_i(g) = [E(s_i).g.E(s_i)]_i$.

That is $E_i(g) = \{(p,x,q) \in E(s_i).g.E(s_i) \mid x \in J_i$, where the product is in $S(\bigcup_{i=1}^{m} J_i)\}$.

Certainly $E_i(g) \subseteq g_i$, otherwise $(s.g.s)_i \not\supseteq g_i$.

Further $E_i(g) = \emptyset$ whenever $E(s_i) = \emptyset$. The latter possibility certainly exists, and as will be seen does not affect the results occurring later in this chapter.

<u>3.12 LEMMA</u> Let $s.s = s \in S(\bigcup_{i=1}^{m} J_i)$, and let $g \in H_s$.

Then $E_i(g) \in H_{E(s_i)}$ for $1 \leq i \leq m$.

<u>Proof</u> : We have $E(s_i).E_i(g) = E(s_i).[E(s_i).g.E(s_i)]_i$. Now $(p,x,q) \in E(s_i).E_i(g)$ implies $(p,x,q) = (p,x_1,r).(r,x_2,t).(t,x_3,q)$ where $(p,x_1,r) \in E(s_i)$, $(r,x_2,t) \in E(s_i)$, $(t,x_2,q) \in g.E(s_i)$, $x_2x_3 \in J_i$ and $x = x_1x_2x_3 \in J_i$. $E(s_i)^2 = E(s_i)$ implies

$(p,x_1x_2,t) \in E(s_i)$ so that $(p,x,q) \in E_i(g)$. Thus $E(s_i).E_i(g) \subseteq E_i(g)$. Now $(p,x,q) \in E_i(g)$ implies $(p,x,q) = (p,x_1,t).(t,x_2,q)$ where $(p,x_1,t) \in E(s_i)$ and $(t,x_2,q) \in g.E(s_i)$, such that $x_1x_2 \in J_i$. But $(p,x_1,t) \in E(s_i)^2$, so that $(p,x_1,t) = (p,x_1',r).(r,x_2',t)$. Now $x = x_1'x_2'x_2 \in J_i$. Thus $J_i = J_{x_2'} \leq J_{x_2'x_2} \leq J_x = J_i$, so that $x_2'x_2 \in J_i$ and $(r,x_2',t).(t,x_2,q) \in E_i(g)$. Hence $(p,x,q) \in E(s_i).E_i(g)$. Thus $E_i(g) = E(s_i).E_i(g)$ and dually $E_i(g) = E_i(g).E(s_i)$.

Also $[E_i(g)]^n = E(s_i).[E_i(g)]^n.E(s_i) = E(s_i).[E(s_i).g.E(s_i)]_i^n.E(s_i)$ $\supseteq E(s_i).\{N[E(s_i)].g.N[E(s_i)]\}_i^n.E(s_i) \supseteq E(s_i).N[E(s_i)].E(s_i) = E(s_i)$. Further $[E(s_i).g.E(s_i)]_i^n \subseteq (s.g.s)_i^n = (g_i)^n \subseteq s_i$. Thus $[E_i(g)]^n \subseteq E(s_i).s_i.E(s_i) \subseteq E(s_i)^2 = E(s_i)$.

Hence $E(s_i) = [E_i(g)]^n$.

Thus $E_i(g) \in H_{E(s_i)}$. #

<u>3.13 LEMMA</u> Let $\{J_1,\ldots,J_n\}$ be a set of $\mathcal{J}$ classes of $S(M)$ such that $J_m \nleq J_i$ for $1 \leq i \leq m-1$.

Let $(x,y) \in (J_m \times \bigcup_{i=1}^{m} J_i) \cup (\bigcup_{i=1}^{m} J_i \times J_m)$

Then $xy \notin \bigcup_{i=1}^{m-1} J_i$.

Proof : Suppose $(x,y) \in J_m \times \bigcup_{i=1}^{m} J_i$ and $xy \in J_i$ for $1 \leq i \leq m - 1$.

Then $J_m = J_x \geq J_{xy} = J_i$, contradicting the assumptions of the lemma.

The case $(x,y) \in \bigcup_{i=1}^{m} J_i \times J_m$ is the dual of the above. #

3.14 LEMMA Let $\{J_1,\ldots,J_m\}$ be a set of distinct $\mathcal{J}$ classes of $S(M)$.

Then there exists $J_i \in \{J_1,\ldots,J_m\}$ such that $J_i \not\geq J_j$ for $j \neq i$ and $1 \leq j \leq m$.

Proof : Suppose this is not the case. Then we may rearrange the set so that $J_k > J_{k+1}$ for $1 \leq k \leq m - 1$. Suppose $J_j > J_k$ for $j > k$. Then we have $J_k > J_{k+1} > \ldots > J_j > J_k$, contradicting the distinctness of the $\mathcal{J}$ classes. But then $J_m > J_\ell$ for some $\ell < m$ which also leads to a contradiction. Therefore there must exist a J_i such that $J_i \not\geq J_j$ for $j \neq i$ and $1 \leq j \leq m$.

3.15 COROLLARY Let $\{J_1,\ldots,J_m\}$ be as above.

Then we may rearrange the set so that $J_i \not\geq J_j$ for $1 \leq j < i \leq m$.

Proof : The result follows by considering successively smaller subsets of $\{J_1,\ldots,J_m\}$. #

3.16 LEMMA Let $s.s = s \in \mathcal{S}(\bigcup_{i=1}^{m} J_i)$, where $\{J_1,\ldots,J_m\}$ is a J-closed set of $\mathcal{J}$ classes of $S(M)$ with $J_m \not\geq J_i$ for $1 \leq i \leq m - 1$.

Define $t(s) = s \setminus s_m = \{(p,x,q) \in s \mid (p,x,q) \notin s_m\}$.

Then $t(s).t(s) = t(s)$ when the product is in $\mathcal{S}(\bigcup_{i=1}^{m-1} J_i)$.

Proof : We have $s = t(s) \cup s_m$.

Thus $s = s^2 = t(s).t(s) \cup t(s).s_m \cup s_m.t(s) \cup s_m^2$, where the products are in $S(\bigcup_{i=1}^{m} J_i)$.

From previous lemmas we know that

$$(p,x,q) \in t(s).s_m \cup s_m.t(s) \cup s_m^2 \text{ implies } x \in J_m.$$

Thus $t(s).s_m \cup s_m.t(s) \cup s_m^2 \subseteq s_m$.

Hence $t(s) \subseteq t(s).t(s) \subseteq s$, and if we consider the product $t(s).t(s)$ in $S(\bigcup_{i=1}^{m-1} J_i)$ we have $t(s) = t(s).t(s)$. From the definitions it can be seen that $\{J_1, --, J_{m-1}\}$ is J-closed. #

3.17 LEMMA Let $s.s = s \in S(\bigcup_{i=1}^{m} J_i)$ where $\{J_1,\ldots,J_m\}$ is as in the previous lemma.

Then $s = s.[t(s) \cup E(s_m)].s$

Proof : Let $s'_m = s_m \setminus E(s_m)$.

Then $s_m = s'_m \cup E(s_m)$ is an element of $S(J_m)$ and there exists $k \in Z^+$ such that s_m^k is an idempotent. Now $s_m^2 = [s'_m \cup E(s_m)]^2 \supseteq E(s_m)^2 = E(s_m)$. Also $s_m^2 \subseteq s_m$ since $s^2 = s$.

Thus $s_m \supseteq s_m^k \supseteq E(s_m)$, and $s_m^k = E(s_m)$ by the definition of $E(s_m)$.

Further $s'^k_m \subseteq s_m^k$, so that $s'^k_m \subseteq E(s_m)$.

We know that $s_m^k \cap t(s) = \emptyset$ when s_m^k is considered as a product in $S(\bigcup_{i=1}^{m} J_i)$.

Also $s = [t(s) \cup E(s_m)] \cup s'_m$.

Thus $s = s^\ell = \{[t(s) \cup E(s_m)] \cup s'_m\}^\ell$ for all $\ell \in Z^+$.

We see that each term in the expansion of this product, except $s_m'^{\ell}$, has $[t(s) \cup E(s_m)]$ as a factor.

Now $[t(s) \cup E(s_m)]^2 \supseteq t(s).t(s) \cup E(s_m)^2 \supseteq t(s) \cup E(s_m)$.

Thus $t(s) \cup E(s_m) \subseteq [t(s) \cup E(s_m)]^3 \subseteq s.[t(s) \cup E(s_m)].s$

Hence each term involving $t(s) \cup E(s_m)$ as a factor must be a subset of $s.[t(s) \cup E(s_m)].s$, since all factors are subsets of s.

Thus $\{[t(s) \cup E(s_m)] \cup s_m'\}^k \subseteq s.[t(s) \cup E(s_m)].s \cup s_m'^k$.

But $s_m'^k \subseteq E(s_m) \subseteq t(s) \cup E(s_m) \subseteq s.[t(s) \cup E(s_m)].s$.

Hence $s \subseteq s.[t(s) \cup E(s_m)].s \subseteq s^3 = s$.

Therefore $s = s.[t(s) \cup E(s_m)].s$. #

3.18 THEOREM Let $s.s = s \in \mathcal{S}(\bigcup_{i=1}^{m} J_i)$, where $\{J_1,\dots,J_m\}$ is a J-closed set of $\mathcal{J}$ classes of $S(M)$ and $J_m \not\geq J_i$ for $1 \leq i \leq m$.

Then $H_s | H_{t(s)} \times H_{E(s_m)}$.

Proof : (i) Let $g \in H_s$. Put $t(g) = g \setminus g_m$; $g_m' = g_m \setminus E_m(g)$.

Then $g = t(g) \cup E_m(g) \cup g_m'$. Suppose $g,h \in H_s$ and consider their product in $\mathcal{S}(\bigcup_{i=1}^{m} J_i)$. We have $g.h =$

$t(g).t(h) \cup t(g).[E_m(h) \cup h_m'] \cup E_m(g).[t(h) \cup h_m'] \cup E_m(g).E_m(h) \cup g_m'.h$.

Now $g.h \setminus t(g).t(h) \subseteq (g.h)_m$.

Thus $t(g).t(h) = t(g.h)$ when the multiplication on the left hand side is in $\mathcal{S}(\bigcup_{i=1}^{m-1} J_i)$, and in $\mathcal{S}(\bigcup_{i=1}^{m} J_i)$ on the right.

Making substitutions in this equation for g and h, we find $t(g) \in H_{t(s)}$ for all $g \in H_s$.

(ii) We have $E_m(g)$ and $E_m(h)$ are both elements of $H_{E(s_m)}$.

Thus $E_m(g).E_m(h) \in H_{E(s_m)}$.

Now $E_m(g).E_m(h) = [E(s_m).g.E(s_m)]_m.[E(s_m).h.E(s_m)]_m$

$$\subseteq [E(s_m).g.E(s_m)^2.h.E(s_m)]_m$$

$$\subseteq [E(s_m).g.h.E(s_m)]_m = E_m(g.h)$$

Thus $[E_m(g).E_m(h)].[E_m(g.h)]^{n-1} \subseteq [E_m(g.h)]^n = E(s_m)$, where $(g.h)^n = s$.

Put $[E_m(g).E_m(h)].[E_m(g.h)]^{n-1} = E'(s_m)$.

We have $E'(s_m) \in H_{E(s_m)}$, since all its factor are in $H_{E(s_m)}$, and thus there exists $k \in Z^+$ such that $E'(s_m)^k = E(s_m)$.

Now $[E'(s_m)]^2 \subseteq E(s_m).E'(s_m) = E'(s_m)$ since $E(s_m)$ is the identity in $H_{E(s_m)}$.

Thus $[E'(s_m)]^k \subseteq E'(s_m)$, and $E(s_m) \subseteq E'(s_m) \subseteq E(s_m)$.

Hence $E(s_m) = E'(s_m)$, and $E_m(g).E_m(h) = \{[E_m(g.h)]^{n-1}\}^{-1} = E_m(g.h)$.

Therefore $E_m(g).E_m(h) = E_m(g.h)$ for all $g,h \in H_s$.

(iii) We have $g = s.g.s = s.t(g).s \cup s.E_m(g).s \cup s.g'_m.s$ for all $g \in H_s$.

But $s.g'_m.s = s.g'_m.s.[t(s) \cup E(s_m)].s$

$$= s.g'_m.s.t(s).s \cup s.g'_m.s.E(s_m).s$$

$$\subseteq s.g'_m.s.t(g^{-1}).t(g).s \cup s.g'_m.s.E_m(g^{-1}).E_m(g).s$$

where all the products are in $S(\bigcup_{i=1}^{m} J_i)$.

Thus $s.g'_m.s \subseteq s.[g.s.g^{-1}].t(g).s \cup s.[g.s.g^{-1}].E_m(g).s$

$= s.t(g).s \cup s.E_m(g).s.$

Hence $g = s.[t(g) \cup E_m(g)].s$ for all $g \in H_s$.

(iv) Consider the map $\psi : H_s \to H_{t(s)} \times H_{E(s_m)}$ defined by :

$$\psi : g \mapsto (t(g), E_m(g)) \quad \text{for all } g \in H_s.$$

The map is an homomorphism ((i) & (ii)), and is 1:1 (iii).

Thus $H_s | H_{t(s)} \times H_{E(s_m)}$. #

<u>3.19 THEOREM</u> Let $s.s = s \in S(\bigcup_{i=1}^{m} J_i)$, where the J_i are as in the previous theorem.

Then $H_s | \prod_{i=1}^{m} H_{E(s_i)}$.

<u>Proof</u> : Arrange the set $\{J_1,\ldots,J_m\}$ so that $J_i \not\leq J_j$ for $1 \leq j < i \leq m$.

Define $t_k(s) = s \setminus \bigcup_{i=k+1}^{m} s_i$, for $1 \leq k \leq m-1$; $t_m(s) = s$.

Then we have $t_k(s).t_k(s) = t_k(s)$ when the multiplication is in $S(\bigcup_{i=1}^{k} J_i)$.

From the previous theorem $H_{t_k(s)} | H_{t_{k-1}(s)} \times H_{E(s_k)}$ for $1 \leq k \leq m$.

Using the transitivity of division of semigroups we have

$$H_s | H_{t_1(s)} \times \prod_{i=2}^{m} H_{E(s_i)}.$$

Now $t_1(s).t_1(s) = t_1(s)$ in $S(J_1)$, and $t_1(s) \supseteq E(s_1)$.

Thus $t_1(s) = E(s_1)$.

Hence $H_s \mid \prod_{i=1}^{m} H_{E(s_i)}$. #

<u>3.20 REMARK</u> As was mentioned in (3.11), for $s.s = s \in S(\bigcup_{i=1}^{m} J_i)$, some of the $E(s_i)$ defined in (3.2) may be empty. It can be seen that in this case the preceding results are :

(3.17) Let $E(s_m) = \emptyset$, $J_m \not\leq J_i$ for $1 \leq i \leq m - 1$.

Then $s = s.t(s).s$.

(3.18) $H_s \mid H_{t(s)}$.

(3.19) $H_s \mid \prod_{i=1}^{m} H_{E(s_i)}$, where we may take $H_{E(s_i)}$ to be the group with only one element whenever $E(s_i) = \emptyset$, so that these factors have no effect in the product.

<u>3.21 THEOREM</u> Let $s^2 = s \in S(M)$.

Then $H_s \mid \prod_{i=1}^{\ell} H_{s_i'}$,

where $s_i'.s_i' = s_i' \in S(J_i')$, for a set $\{J_1', \ldots, J_\ell'\}$ of J classes of $S(M)$, such that $(p,x,q) \in s$ implies $x \in J_i'$ for some i such that $1 \leq i \leq \ell$, and for each i such that $1 \leq i \leq \ell$ there exists $(p,x,q) \in s$ such that $x \in J_i'$.

<u>Proof</u> : Let $\{J_1, \ldots, J_n\}$ be ~~the~~ a J-closed set of J classes of $S(M)$ such that for any $g \in H_s$ and $(p,x,q) \in g$ there exists $1 \leq i \leq m$ such that $x \in J_i$. ~~and for any J_i in the set there exists $g \in H_s$ and $(p,x,q) \in g$ such that $x \in J_i$~~. This set will in general be larger than the set defined in the statement of the theorem.

Now any group elements of H_s in $S(M)$ may be considered as elements of $S(\bigcup_{i=1}^{n} J_i)$. Further the product of any two elements of H_s is also an element of $S(\bigcup_{i=1}^{n} J_i)$, since it is an element of H_s. Certainly any element of H_s, the H class of s in $S(M)$, is also an element of H'_s the H class of s in $S(\bigcup_{i=1}^{n} J_i)$ when s is considered as an element of the latter semigroup, as is the group element referred to. Thus we see that H_s is isomorphic to a subgroup of H'_s.

From the previous theorem we have that

$$H'_s \mid \prod_{j=1}^{n} H_{E(s_j)} ,$$

and that $\prod_{j=1}^{n} H_{E(s_j)} \mid \prod_{i=1}^{\ell} H_{s'_i}$, where $s'_i . s'_i = s'_i \in S(J'_i)$ and $s'_i = E(s_j)$ when $J'_i = J_j$, for $1 \leq i \leq \ell$. We have deleted the terms of the product where $E(s_j) = \emptyset$ and $J_j \notin \{J'_1,\ldots,J'_\ell\}$, since in these cases $H_{E(s_j)}$ may be considered as the group with one element and trivially divides any other group. Certainly $E(s_j) = \emptyset$ whenever $J_j \notin \{J'_1,\ldots,J'_\ell\}$.

Thus $H_s \mid H_{s'} \mid \prod_{j=1}^{n} H_{E(s_j)} \mid \prod_{i=1}^{\ell} H_{s'_i}$.

Hence $H_s \mid \prod_{i=1}^{\ell} H_{s'_i}$. #

<u>3.22 REMARK</u> The product $\prod_{i=1}^{\ell} H_{s'_i}$ defined in the previous theorem may be further reduced by noticing that it is possible that $E(s_j) = \emptyset$ when $J_j = J'_i$. In this case we may adopt the

convention that $H_{s'_i}$ is the group with one element. In fact the result will remain true for any $s'_i.s'_i = s'_i \varepsilon S(J_i)$ in this case. This will not affect further results since we deal in the next chapters with all the subgroups of all the $S(J)$ for J a J class of $S(M)$.

CHAPTER 4. THE SUBGROUPS of the SEMIGROUPS $\mathcal{S}(J)$.

4.1 REMARK From the previous chapter we know that any simple group dividing $\mathcal{S}(M)$ must divide the direct product of subgroups of semigroups of type $\mathcal{S}(J)$. Thus any simple group dividing $\mathcal{S}(M)$ divides a subgroup of $\mathcal{S}(J)$ for some $\mathcal{J}$ class J of $S(M)$.

In this chapter it is shown that the subgroup of $\mathcal{S}(J)$ associated with an idempotent, s, of $\mathcal{S}(J)$ divides a direct product of a set of subgroups of $\mathcal{S}(J)$ associated with idempotents of $\mathcal{S}(J)$ which are subsets of s. These idempotents have the following properties : suppose t is such an idempotent, then;

(i) $t = N(t).t.N(t)$

(ii) if $w,w' \in N(t)$ such that $w \neq w'$, then there does not exist $(p,x,q) \in t$ such that $w.(p,x,q).w' = (p,x,q)$.

4.2 LEMMA Let $t \in \mathcal{S}(J)$, where J is a $\mathcal{J}$ class of $S(M)$.

Let $N' \subseteq N(t)$.

Then $N'.N' \supseteq N'$.

Proof : $(q,x,q) \in N'$ implies

$(q,x,q) = (q,x^2,q) = (q,x,q).(q,x,q) \in N'.N'$.

4.3 LEMMA Let $s.s = s \in \mathcal{S}(J)$.

Then $[N(s).s.N(s)]^2 = N(s).s.N(s) \in \mathcal{S}(J)$, and $H_s | H_{N(s).s.N(s)}$.

Proof : Let $g \in H_s$. Then $g.s = g = s.g$.

(i) Suppose $g,h \in H_s$. Then

$N(s).g.N(s).N(s).h.N(s) \subseteq N(s).g.s^2.h.N(s) = N(s).g.h.N(s)$.

But $N(s).g.h.N(s) = N(s).g.s.h.N(s) = N(s).g.s.N(s).s.h.N(s)$

$$= N(s).g.N(s).h.N(s)$$

$$\subseteq N(s).g.N(s).N(s).h.N(s)$$

Thus $[N(s).g.N(s)].[N(s).h.N(s)] = N(s).[g.h].N(s)$ for all $g,h \in H_s$.

In particular $[N(s).s.N(s)]^2 = N(s).s.N(s)$.

(ii) Let $g \in H_s$. Then

$$g = s.g.s = s.N(s).s.g.s.N(s).s = s.[N(s).g.N(s)].s.$$

(iii) Let $g \in H_s$. Then $[N(s).g.N(s)]^n = N(s).s.N(s)$ where $g^n = s$.

also $[N(s).g.N(s)].[N(s).s.N(s)] = N(s).g.N(s)$

and $[N(s).s.N(s)].[N(s).g.N(s)] = N(s).g.N(s)$ (from (i)).

Thus $N(s).g.N(s) \in H_{N(s).s.N(s)}$ for all $g \in H_s$.

(iv) Define a mapping $\psi : H_s \to H_{N(s).s.N(s)}$ by :

$$\psi : g \to N(s).g.N(s) \quad \text{for all } g \in H_s.$$

Then ψ is an homomorphism, from (i), and is 1:1, from (ii).

Thus $H_s | H_{N(s).s.N(s)}$. #

<u>4.4 REMARK</u> Let $s.s = s \in S(J)$.

Suppose $(p,y,q) \in N(s).s.N(s)$.

Then $(p,y,q) = (p,x,p).(p,y',q).(q,z,q)$, where (p,x,p), $(q,z,q) \in N(s)$ and $(p,y',q) \in s$.

Thus $(p,x,p).(p,y,q) = (p,y,q) = (p,y,q).(q,z,q)$.

That is, for all $(p,y,q) \varepsilon N(s).s.N(s)$, there exist $w,v \varepsilon N(s)$ such that $w.(p,y,q) = (p,y,q) = (p,y,q).v$.

4.5 REMARK For the remainder of the chapter, only idempotents of $S(J)$ which have this property will be considered, except where stated. That is if $s.s = s \varepsilon S(J)$ then for all $(p,y,q) \varepsilon s$, there exist $w,v \varepsilon N(s)$ such that $w.(p,y,q) = (p,y,q) = (p,y,q).v$.

We see that for such idempotents

$$s = s.N(s) = N(s).s = N(s).s.N(s).$$

4.6 DEFINITION Let $t \varepsilon S(\bigcup_{i=1}^{m} J_i)$, where $\{J_1,\ldots,J_m\}$ is any $\mathcal{J}$-closed set of $\mathcal{J}$ classes of $S(M)$.

Let $w = (q,x,q) \varepsilon T(M)$, such that $x^2 = x$.

Then

(i) $w(t) = \{(q,y,q) \varepsilon t \mid y \; H \; x\}$

(ii) $Dw(t) = \{(q,y,q') \varepsilon t \setminus w(t) \mid y \; R \; x\}$

(iii) $Sw(t) = \{(q',y,q) \varepsilon t \setminus w(t) \mid y \; L \; x\}$

(iv) $Nw(t) = t \setminus [w(t) \cup Dw(t) \cup Sw(t)]$.

4.7 REMARK It is easily seen that these subsets of t are mutually disjoint. For suppose $(p,y,p') \varepsilon Dw(t) \cap Sw(t)$. Then $(p,y,p') = (q,y,q)$ and $y \; R \; x$ and $y \; L \; x$, so that $y \; H \; x$. Thus $(p,y,p) \varepsilon w(t)$, which contradicts $Dw(t) \subseteq t \setminus w(t)$. Thus $Dw(t) \cap Sw(t) = \emptyset$.

Certainly $t = w(t) \cup Dw(t) \cup Sw(t) \cup Nw(t)$, for any w of the form given.

Notice that $w(t) \cup Dw(t) \cup Sw(t)$ may be considered as an element of $S(J)$, where $J = J_x$ for $w = (q,x,q)$.

Further the concepts $Dw(t)$ and $Sw(t)$ are dual, and $w(t)$ and $Nw(t)$ are each self dual.

<u>4.8 LEMMA</u> Let $s,t \in \mathcal{S}(J)$, and let $w = (q,x,q)$ such that $x^2 = x$ and $J = J_x$.

Then

(i) $w(s.t) = w(s).w(t) \cup w(s).Sw(t) \cup Dw(s).Sw(t) \cup Dw(s).w(t)$

(ii) $Dw(s.t) = Dw(s).Nw(t) \cup Dw(s).Dw(t) \cup w(s).Nw(t) \cup w(s).Dw(t)$

(iii) $Sw(s.t) = Sw(s).w(t) \cup Sw(s).Sw(t) \cup Nw(s).w(t) \cup Nw(s).Sw(t)$

(iv) $Nw(s.t) = Nw(s).Nw(t) \cup Nw(s).Dw(t) \cup Sw(s).Nw(t) \cup Sw(s).Dw(t)$.

<u>Proof</u> : Suppose $(q',y,q'') \in w(s).w(t) \cup w(s).Sw(t) \cup Dw(s).w(t) \cup Dw(s).Sw(t)$.

Then $(q',y,q'') = (q,y_1,q_1).(q_1,y_2,q)$ where $y_1 \mathcal{R} x$ and $y_2 \mathcal{L} x$, since $(q,y_1,q_1) \in w(s) \cup Dw(s)$ implying $y_1 \mathcal{H} x$ or $y_1 \mathcal{R} x$, and $(q_1,y_2,q) \in w(t) \cup Sw(t)$ implying $y_2 \mathcal{H} x$ or $y_2 \mathcal{L} x$.

Now $y_1 y_2 = y \in J_x$, since the product~~s~~ ~~of which~~ (q',y,q'') is ~~one are~~ in $\mathcal{S}(J)$. Thus from lemma 2.9 we have that $y \mathcal{H} x$. Hence $(q',y,q'') \in w(s.t)$, for all terms on the right are in $s.t$.

Thus $w(s.t) \subseteq w(s).w(t) \cup w(s).Sw(t) \cup Dw(s).w(t) \cup Dw(s).Sw(t)$.

Similarly we may show such an inclusion for the remaining parts of the statement. Since the terms on the right of the equations exhaust the terms of the expanded product of s and t, we must have equality rather than inclusion in each of the four parts of the statement. #

<u>4.9 LEMMA</u> Let $t \in \mathcal{S}(\bigcup_{i=1}^{m} J_i)$, where $\{J_1,\ldots,J_m\}$ is any J-closed set of $\mathcal{J}$ classes of $S(M)$.

Let $w = (q,x,q) \in T(M)$, such that $x^2 = x$.

Then

(i) $w.w(t) = w(t).w = w(t)$

(ii) $w.Dw(t) = Dw(t)$

(iii) $Sw(t).w = Sw(t)$.

Proof : The result is a corollary of lemma 2.10.

4.10 LEMMA Let $s.s = s \in S(J)$. Let $w \in N(s)$, such that $w(s) \subseteq Dw(s).Sw(s)$.

Then

$$[Nw(s)]^2 = Nw(s) \in S(J), \text{ and } H_s | H_{Nw(s)} .$$

Proof : (i) Let $g,h \in H_s$. Then $g.s = g = s.g$.

Now

$$Nw(g.h) = Nw(g).Nw(h) \cup Nw(g).Dw(h) \cup Sw(g).Nw(h) \cup Sw(g).Dw(h)$$

We have

$$Dw(h) = w.Dw(h) \subseteq w(s).Dw(h) \subseteq Dw(s).Sw(s).Dw(h) \subseteq Dw(s).Nw(h)$$

Thus $[Nw(g) \cup Sw(g)].Dw(h) \subseteq [Nw(g) \cup Sw(g)].Dw(s).Nw(h)$

$\subseteq [Nw(g).Dw(s) \cup Sw(g).Dw(s)].Nw(h)$

$\subseteq Nw(g).Nw(h)$.

Also

$$Sw(g) = Sw(g).w \subseteq Sw(g).w(s) \subseteq Sw(g).Dw(s).Sw(s) \subseteq Nw(g).Sw(s).$$

Thus $Sw(g).Nw(h) \subseteq Nw(g).Sw(s).Nw(h) \subseteq Nw(g).Nw(h)$.

Hence $Nw(g.h) = Nw(g).Nw(h)$, for all $g,h \in H_s$.

In particular $Nw(s) = [Nw(s)]^2$, and $Nw(s) \subseteq s \in S(J)$ so that $Nw(s) \in S(J)$.

(ii) Let $g \in H_s$.

We have $Dw(s).Nw(g) \subseteq Dw(g)$ and $Nw(g).Sw(s) \subseteq Sw(g)$.

Thus $Dw(s).Nw(g) = Dw(g)$

and $Nw(g).Sw(s) = Sw(g)$, from the reverse inclusions proven in (i).

Also $w(g) = w(g).w \subseteq w(g).w(s) \subseteq w(g).Dw(s).Sw(s)$

$\subseteq Dw(g).Sw(s) = Dw(s).Nw(g).Sw(s)$,

and $Dw(s).Nw(g).Sw(s) \subseteq Dw(g).Sw(s) \subseteq w(g)$.

Thus $g = Dw(s).Nw(g).Sw(s) \cup Dw(s).Nw(g) \cup Nw(g).Sw(s) \cup Nw(g)$, for all $g \in H_s$.

(iii) We have $Nw(g).Nw(g^{-1}) = Nw(s) = Nw(g^{-1}).Nw(g)$

and $Nw(g).Nw(s) = Nw(g) = Nw(s).Nw(g)$ for all $g \in H_s$.

Thus $Nw(g) \in H_{Nw(s)}$.

(iv) Define a mapping $\psi : H_s \to H_{Nw(s)}$ by :

$$\psi : g \mapsto Nw(g) \quad \text{for all } g \in H_s .$$

We know that ψ is an homomorphism, (i), and is 1:1, (ii).

Thus $H_s | H_{Nw(s)}$. #

4.11 REMARK (a) Suppose $w = (q,x,q)$ and $v = (q,y,q)$ such that $x^2 = x$, $y^2 = y$, $x \mathcal{L} y$ and $x \neq y$. Then $w.v = w$ and $v.w = v$, from lemma 2.10 (ii). Further $z \mathcal{L} x$ iff $z \mathcal{L} y$, so that $Sw(t) = Sv(t)$ for all $t \in \mathcal{S}(M)$. Now $x \neq y$ implies $x \not\mathcal{R} y$, and $Dw(t) \cap Dv(t) = \emptyset$, for all $t \in \mathcal{S}(M)$.

Suppose $s^2 = s \in \mathcal{S}(J)$ and $w,v \in s$. Then we have $v(s) \subseteq Sw(s)$, and $w(s) \subseteq Sv(s)$. Also

$w(s).v(s) \subseteq w(s).Sw(s) \subseteq w(s) = w(s).w = w(s).w.v = (w(s).w).v$ $= w(s).v \subseteq w(s).v(s)$. Thus $w(s).v(s) = w(s)$, and similarly $v(s).w(s) = v(s)$.

(b) Dually if $w = (q,x,q), v = (q,y,q)$ and $x^2 = x$, $y^2 = y$, $x \neq y$ and $x \mathcal{R} y$, then $Dw(t) = Dv(t)$, $Sw(t) \cap Sv(t) = \emptyset$ for all $t \in \mathcal{S}(M)$. Also for $s^2 = s \in \mathcal{S}(J)$ where $w,v \in s$ we have $w(s).v(s) = v(s)$ and $v(s).w(s) = w(s)$.

This remark motivates the following lemma.

<u>4.12 LEMMA</u> Let $s.s = s \in \mathcal{S}(J)$.

(i) Let $w,v \in N(s)$ such that $w \neq v$ and $w.v = w$, $v.w = v$. Then $Nw(s) \cup Sw(s)$ is an idempotent in $\mathcal{S}(J)$, and $H_s | H_{Nw(s) \cup Sw(s)}$.

(ii) Let $w,v \in N(s)$ such that $w \neq v$ and $w.v = v$, $v.w = w$. Then $Nw(s) \cup Dw(s)$ is an idempotent in $\mathcal{S}(J)$, and $H_s | H_{Nw(s) \cup Dw(s)}$.

<u>Proof</u> : (i) (a) Let $g,h \in H_s$.

Then $Sw(g.h) = Sw(g).Sw(h) \cup Nw(g).Sw(h) \cup [Sw(g) \cup Nw(g)].w(h)$

Now

$$w(h) = w.w(h) \subseteq w(s).w(h) = w(s).v(s).w(h) \subseteq w(s).Sw(s).w(h) \subseteq w(s).Sw(h).$$

Thus
$$\begin{aligned}[Sw(g) \cup Nw(g)].w(h) &\subseteq [Sw(g) \cup Nw(g)].w(s).Sw(h) \\ &= [Sw(g).w(s) \cup Nw(g).w(s)].Sw(h) \\ &\subseteq Sw(g).Sw(h).\end{aligned}$$

Hence $Sw(g.h) = Sw(g).Sw(h) \cup Nw(g).Sw(h)$.

Further

$$Nw(g.h) = Nw(g).Nw(h) \cup Sw(g).Nw(h) \cup [Nw(g) \cup Sw(g)].Dw(h).$$

Now $Dw(h) = w.Dw(h) \subseteq w(s).Dw(h) = w(s).v(s).Dw(h)$

$$\subseteq w(s).Nw(h).$$

Thus $[Nw(g) \cup Sw(g)].Dw(h) \subseteq [Nw(g) \cup Sw(g)].w(s).Nw(h)$

$$\subseteq Sw(g).Nw(h).$$

Hence $Nw(g.h) = Nw(g).Nw(h) \cup Sw(g).Nw(h)$.

Combining these results we find

$$Nw(g.h) \cup Sw(g.h) = [Nw(g) \cup Sw(g)].[Nw(h) \cup Sw(h)],$$

for all $g,h \in H_s$. In particular for $g = h = s$.

(b) Further for $g \in H_s$ we have :

$w(g) \subseteq w(s).Sw(g) \subseteq w(g)$, and $Dw(g) \subseteq w(s).Nw(g) \subseteq Dw(g)$.

Thus $w(g) = w(s).Sw(g)$ and $Dw(g) = w(s).Nw(g)$.

Hence $g = w(s).Sw(g) \cup w(s).Nw(g) \cup Sw(g) \cup Nw(g)$.

(c) From part (a) we see by substituting for g and h that

$$Sw(g) \cup Nw(g) \in H_{Sw(s) \cup Nw(s)}, \text{ for all } g \in H_s.$$

(d) Define a mapping $\psi : H_s \to H_{Sw(s) \cup Nw(s)}$ by :

$$\psi : g \mapsto Sw(g) \cup Nw(g), \text{ for all } g \in H_s.$$

The map is a monomorphism ((a) & (b)).

Thus $H_s | H_{Sw(s) \cup Nw(s)}$.

(ii) This is the dual of part (i). #

4.13 REMARK The two preceding lemmas may be summarized as follows :

Let $s.s = s \in \mathcal{S}(J)$. Then $H_s | H_{s'}$ where $s'.s' = s' \in \mathcal{S}(J)$ and

(i) for all $v,w \in N(s')$, $w \notin Sv(s') \cup Dv(s')$ (4.12)

(ii) for all $w \in N(s')$, $Dw(s').Sw(s') = \emptyset$ (4.10)

The first condition follows from the remarks 4.11.

The second may be seen to be equivalent to the conditions of (4.10) by supposing there exists $(q,y,q) \in Dw(s').Sw(s')$. Then $(q,y,q) \in w(s')$. We have $w(s') \subseteq w(s').w(s') \subseteq w(s').w = w(s')$. Hence $w(s') = w(s').w(s')$ and the set $\{z \in H_x | (q,z,q) \in w(s')\}$ must be a subgroup of H_x. Hence $w(s').(q,y,q) = w(s')$. Then $w(s') = w(s').(q,y,q) \subseteq w(s').Dw(s').Sw(s') \subseteq Dw(s').Sw(s')$. That is $w(s') \subseteq Dw(s').Sw(s')$. We have assumed $w = (q,x,q)$.

Hence if $Dw(s').Sw(s') \neq \emptyset$ for some $w \in N(s)$, then $H_{s'} | H_{Nw(s')}$. Only when $Dw(s').Sw(s') = \emptyset$ for all $w \in N(s)$ will (4.10) be inapplicable to $H_{s'}$.

All idempotents in $\mathcal{S}(J)$ considered in the remainder of this chapter will be assumed to satisfy the properties (i) and (ii), [as well as (4.5)], except where otherwise stated.

<u>4.14 DEFINITION</u> Let $t \in \mathcal{S}(J)$. Let $w = (q,x,q)$, $v = (p,y,p)$ such that $w,v \in T(M)$ and $x^2 = x$, $y^2 = y$.

Define $DSwv(t) = \{Dw(t) \cup w(t)\} \cap \{Sv(t) \cup v(t)\}$.

The dual of $DSwv(t)$ is $DSvw(t)$.

<u>4.15 LEMMA</u> Let $s.s = s \in \mathcal{S}(J)$.

(i) Let $w \in N(s)$ and let $g \in H_s$. Then there exist $v_1,v_2 \in N(s)$ such that $DSwv_1(g) \neq \emptyset$ and $DSv_2w(g) \neq \emptyset$.

(ii) Let $w, w_1, w_2 \in N(s)$, and let $g, h \in H_s$. Then $DSww_1(g).DSw_1w_2(h) \subseteq DSww_2(g.h)$, and $DSww_1(g) \neq \emptyset$ and $DSw_1w_2(h) \neq \emptyset$ implies $DSww_2(g.h) \neq \emptyset$.

Proof : (i) From (4.5) we have that $s = N(s).s = s.N(s)$. Thus $g \in H_s$ implies $g = s.g.s = N(s).s.g.s.N(s) = N(s).g.N(s)$.

Suppose $w \in N(s)$. Then
$w \in w(s) = w(g.g^{-1}) = [Dw(g) \cup w(g)].[Sw(g^{-1}) \cup w(g^{-1})]$. Thus
$w(s) \neq \emptyset$ implies $Dw(g) \cup w(g) \neq \emptyset$. Suppose
$(p,y,q) \in Dw(g) \cup w(g)$. Then $(p,y,q) \in N(s).g.N(s)$. There must exist $v_1 \in N(s)$ such that $(p,y,q) = w.(p,z,q).v_1$ where $(p,z,q) \in g$. Hence $(p,y,q) = w.(p,y,q).v_1$. Now $y = xyx_1$, where $w = (p,x,p)$, $v_1 = (q,x_1,q)$. Thus $xyx_1 \in J$ and $xyx_1 \; L \; x_1$. Hence $(p,y,q) \in Sv_1(g) \cup v_1(g)$. Thus $(p,y,q) \in DSwv_1(g)$. That is $DSwv_1(g) \neq \emptyset$.

The other part is the dual of this.

(ii) Suppose $w = (q,x,q)$, $w_1 = (q_1,x_1,q_1)$, $w_2 = (q_2,x_2,q_2)$. Let $(q,y_1,q_1) \in DSww_1(g)$ and $(q_1,y_2,q_2) \in DSw_1w_2(h)$. Then $y_1 \; L \; x_1$ and $y_2 \; R \; x_1$, so that $Z(y_1) = Z(x_1)|P(x_1) = P(y_2)$. Hence $y_1y_2 \in J$ and $y_1y_2 \; R \; y_1 \; R \; x$ and $y_1y_2 \; L \; y_2 \; L \; x_2$. Certainly $(q,y_1\,y_2,q_2) \in g.h$. Thus $(q,y_1\,y_2,q_2) \in DSww_2(g.h)$. It follows that $DSww_1(g).DSw_1w_2(h) \subseteq DSww_2(g.h)$. Certainly if either of $DSww_1(g)$ or $DSw_1w_2(g)$ is empty then the result is trivially true. The other part also follows from this proof. #

4.16 LEMMA Let $s.s = s \in S(J)$, not necessarily satisfying the conditions of (4.5) and (4.13).

Let $N' \subseteq N(s)$ such that $DSww'(s) \neq \emptyset$ for all $(w,w') \in N' \times N'$.

Then if $|N'| > 1$, $Dw(s).Sw(s) \neq \emptyset$ for all $w \in N'$.

Proof : Let $w, w' \in N'$, such that $w \neq w'$ (i.e. $|N'| \geq 1$). Then $DSww'(s) \neq \emptyset$ and $DSw'w(s) \neq \emptyset$. From the previous lemma we see that $DSww'(s).DSw'w(s) \neq \emptyset$. Now $Dw(s) \supseteq DSww'(s)$, and $Sw(s) \supseteq DSw'w(s)$. Thus $Dw(s).Sw(s) \neq \emptyset$. #

4.17 COROLLARY Let $s.s = s \in S(J)$, satisfying the conditions of (4.5) and (4.13).

Let $w, w' \in N(s)$ such that $w \neq w'$.

Then $DSww'(s) \neq \emptyset$ implies $DSw'w(s) = \emptyset$.

Proof : Suppose not. Then $\{w, w'\} \subseteq N(s)$ satisfies the conditions of the previous lemma, and s would not satisfy 4.13 (ii). #

4.18 DEFINITION Let $t.t = t \in S(J)$ satisfying the conditions of (4.5) and (4.13).

Define

(i) $L(t) = \{w \in N(t) \mid DSwv(t) = DSvw(t) = \emptyset$ for all $v \in N(s)$ such that $w \neq v\}$

(ii) $I(t) = \{w \in N(t) \setminus L(t) \mid DSvw(t) = \emptyset$ for all $v \in N(s)$ such that $w \neq v\}$

(iii) $T(t) = \{w \in N(t) \setminus L(t) \mid DSwv(t) = \emptyset$ for all $v \in N(s)$ such that $w \neq v\}$

(iv) $R(t) = N(t) \setminus [L(t) \cup I(t) \cup T(t)]$

We see that these subsets of $N(t)$ are mutually disjoint.

Also $L(t)$ and $R(t)$ are each self-dual concepts, and $I(t)$ and $T(t)$ are dual concepts.

<u>4.19 LEMMA</u> Let $s.s = s \in S(J)$. Let $g \in H_s$.

(i) Let $w \in L(s) \cup T(s)$ and let $w_1 \in N(s)$ such that $DSww_1(g) \neq \emptyset$. Then $w_1 \in L(s) \cup T(s)$.

(ii) Let $w \in L(s) \cup I(s)$ and let $w_1 \in N(s)$ such that $DSw_1w(g) \neq \emptyset$. Then $w_1 \in L(s) \cup I(s)$.

<u>Proof</u> : (i) Suppose there exists $w_2 \in N(s)$ such that $DSw_1w_2(s) \neq \emptyset$. From lemma 4.15 (i) we know there exists $w_3 \in N(s)$ such that $DSw_2w_3(g^{-1}) \neq \emptyset$. Thus
$DSww_3(s) \supseteq DSww_1(g).DSw_1w_2(s).DSw_2w_3(g^{-1}) \neq \emptyset$. But
$w \in L(s) \cup T(s)$ implies $w_3 = w$. Then
$DSw_2w_1(s) \supseteq DSw_2w(g^{-1}).DSww_1(g) \neq \emptyset$. From (4.17) we know this is a contradiction to 4.13 (ii), unless $w_2 = w_1$. Thus
$DSw_1w_2(s) = \emptyset$ whenever $w_1 \neq w_2$. Thus $w_1 \in L(s) \cup T(s)$.

(ii) This is the dual of part (i). #

<u>4.20 LEMMA</u> Let $s.s = s \in S(J)$, and let $g \in H_s$.

(i) Let $w \in L(s)$ and $w_1 \in N(s)$ such that $DSww_1(g) \neq \emptyset$. Then $w_1 \in L(s)$.

(ii) Let $w \in L(s)$ and $w_1 \in N(s)$ such that $DSw_1w(g) \neq \emptyset$. Then $w_1 \in L(s)$.

<u>Proof</u> : (i) Suppose $DSw_2w_1(s) \neq \emptyset$ for $w_2 \in N(s)$. There exists $w_3 \in N(s)$ such that $DSw_1w_3(g^{-1}) \neq \emptyset$. Thus
$DSww_3(s) \neq \emptyset$, so that $w_3 = w$. Further, there exists $w_4 \in N(s)$ such that $DSw_4w_2(g) \neq \emptyset$. Thus
$DSw_4w(s) \supseteq DSw_4w_2(g).DSw_2w_1(s).DSw_1w(g^{-1}) \neq \emptyset$. Thus $w_4 = w$.
Also $DSw_1w_2(s) \supseteq DSw_1w(g^{-1}).DSww_2(g) \neq \emptyset$. This contradicts our

supposition, unless $w_2 = w_1$. Thus $w_1 \in L(s) \cup I(s)$. From the previous lemma we know that $w_1 \in L(s) \cup T(s)$. Hence $w_1 \in L(s)$.

(ii) This is the dual of part (i). #

4.21 COROLLARY Let $s.s = s \in S(J)$, and let $g \in H_s$.

Then

(i) $w \in T(s)$ implies $w_1 \in T(s)$ whenever $w_1 \in N(s)$ and $DSww_1(g) \neq \emptyset$.

(ii) $w \in I(s)$ implies $w_1 \in I(s)$ whenever $w_1 \in N(s)$ and $DSw_1w(g) \neq \emptyset$.

Proof : (i) $DSww_1(g) \neq \emptyset$ implies $w_1 \in L(s) \cup T(s)$. Suppose $w_1 \in L(s)$. From the previous lemma we have $w \in L(s)$. Thus $w \notin T(s)$. Hence $w_1 \in T(s)$.

(ii) The dual of (i). #

4.22 REMARK We summarize the results above as follows.

Let $s.s = s \in S(J)$, and let $g \in H_s$.

Then

(i) $w \in L(s)$ implies $w_1 \in L(s)$ whenever $w_1 \in N(s)$ and $DSww_1(g) \neq \emptyset$ or $DSw_1w(g) \neq \emptyset$.

(ii) $w \in T(s)$ implies $w_1 \in T(s)$ whenever $w_1 \in N(s)$ and $DSww_1(g) \neq \emptyset$.

(iii) $w \in I(s)$ implies $w_1 \in I(s)$ whenever $w_1 \in N(s)$ and $DSw_1w(g) \neq \emptyset$.

4.23 LEMMA Let $s.s = s \in S(J)$. Let $g \in H_s$. Let $N_1, N_2 \subseteq N(s)$.

Then

(i) $N_1.g.N_1 = \{(p,x,q) \in g | (p,x,q) \in DSw_1w_2(g)$ where $(w_1,w_2) \in N_1 \times N_2\}$

(ii) $g = N(s).g.N(s)$.

<u>Proof</u> : (i) Suppose $(p,x,q) \in DSw_1w_2(g)$ for $(w_1,w_2) \in N_1 \times N_2$. Then $w_1.(p,x,q).w_2 = (p,x,q)$, and $(p,x,q) \in N_1.g.N_2$.

Conversely if $(p,x,q) \in N_1.g.N_2$ then there exists $(w_1,w_2) \in N_1 \times N_2$ such that $(p,x,q) = w_1.(p,y,q).w_2$ for some $(p,y,q) \in g$. Suppose $w_1 = (p,x_1,p)$, $w_2 = (q,x_2,q)$. Then $x = x_1yx_2$, and $x_1yx_2 \mathcal{R} x_1$ and $x_1yx_2 \mathcal{L} x_2$. Hence $(p,x,q) \in DSw_1w_2(g)$.

(ii) Demonstrated in the proof of (4.15). #

<u>4.24 LEMMA</u> Let $s.s = s \in S(J)$. Let $N_1,N_2 \subseteq N(s)$, such that $N_1 \cap N_2 = \emptyset$. Then $N_1.s \cap N_2.s = \emptyset$ and $s.N_1 \cap s.N_2 = \emptyset$.

<u>Proof</u> : Let $(p,x,q) \in N_1.s \cap N_2.s$. Then there exist $(w_1,w_2) \in N_1 \times N_2$ such that $w_1.(p,y_1,q) = w_2.(p,y_2,q) = (p,x,q)$, where (p,y_1,q), $(p,y_2,q) \in s$. Suppose $w_1 = (p,x_1,p)$ and $w_2 = (p,x_2,p)$. Then $x_1 \mathcal{R} x_1y_1 = x = x_2y_2 \mathcal{R} x_2$, and $x_1 \mathcal{R} x_2$, contradicting condition 4.13 (i). Thus $N_1.s \cap N_2.s = \emptyset$. The second part is the dual of the first. #

<u>4.25 LEMMA</u> Let $s.s = s \in S(J)$.

Then

(i) $L(s).g.(IUTUR)(s) = (IUTUR)(s).g.L(s) = \emptyset$ for all $g \in H_s$.

(ii) $L(s).(IUTUR)(s) = (IUTUR)(s).L(s) = \emptyset$.

[Here $(IUTUR)(s) = I(s) \cup T(s) \cup R(s)$.]

Proof :

(i) $L(s).g.(IUTUR)(s) = \{ \bigcup_{(w_1,w_2)\varepsilon A} DSw_1w_2(g) \mid A = L(s) \times (IUTUR)(s)\}$,

for all $g \varepsilon H_s$. But $DSw_1w_2(g) = \emptyset$ whenever $w_1 \varepsilon L(s)$ and $w_2 \notin L(s)$. Now $L(s) \cap (IUTUR)(s) = \emptyset$. Thus $L(s).g.(IUTUR)(s) = \emptyset$. The other part is the dual of this.

(ii) $L(s).(IUTUR)(s) \subseteq L(s).L(s).(IUTUR)(s) \subseteq L(s).s.(IUTUR)(s) = \emptyset$.

[$L(s) \subseteq L(s).L(s)$ from (4.2)].

The other part is the dual of this. #

4.26 COROLLARY Let $s.s = s \varepsilon S(J)$. Let $g \varepsilon H_s$.

Then $g \neq L(s).g.L(s) \cup (IUTUR)(s).g.(IUTUR)(s)$.

Proof : $g = N(s).g.N(s) = [L(s) \cup (IUTUR)(s)].g.[L(s) \cup (IUTUR)(s)]$

$= L(s).g.L(s) \cup (IUTUR)(s).g.(IUTUR)(s)$. #

4.27 DEFINITION Let $s.s = s \varepsilon S(J)$, and $g \varepsilon H_s$.

Define

(i) $LP(g) = L(s).g.L(s)$

(ii) $RP(g) = (IUTUR)(s).g.(IUTUR)(s)$.

4.28 LEMMA Let $s.s = s \varepsilon S(J)$, such that $RP(s) \neq \emptyset$.

Then (i) $I(s) \neq \emptyset$,

(ii) $T(s) \neq \emptyset$,

(iii) $L(s) = N(LP(s))$,

(iv) $(IUTUR)(s) = N(RP(s))$.

Proof : (i) Suppose $I(s) = \emptyset$. Then for all $w \varepsilon N(s) \setminus L(s)$, there exists $w' \varepsilon N(s) \setminus L(s)$ such that $DSw'w(s) \neq \emptyset$. Choose $w_1 \varepsilon N(s) \setminus L(s)$. There exists $w_2 \varepsilon N(s) \setminus L(s)$ such that

$DSw_2w_1(s) \neq \emptyset$. We may find a sequence $\{w_1, w_2, \ldots, w_n\} \subseteq N(s) \setminus L(s)$ such that $DSw_{i+1}w_i(s) \neq \emptyset$ for $1 \leq i \leq n-1$, for all $n \in Z^+$. But $N(s) \setminus L(s)$ is finite, thus there exists $w_k = w_j$ for some $k \gneq j$. Applying lemma 4.15 we have $DSw_jw_{k-1}(s) \neq \emptyset$ and $DSw_{k-1}w_k(s) = DSw_{k-1}w_j(s) \neq \emptyset$, contradicting the condition of 4.13 (ii). Thus $I(s) \neq \emptyset$.

(ii) This is the dual of part (i).

(iii) & (iv) We have $L(s) \subseteq L(s).L(s).L(s) \subseteq L(s).s.L(s) = LP(s)$.

Thus $L(s) \subseteq N(LP(s))$.

Also $(IUTUR)(s) \subseteq (IUTUR)(s)^3 \subseteq (IUTUR)(s).s.(IUTUR)(s) \subseteq RP(s)$.

Thus $(IUTUR)(s) \subseteq N(RP(s))$.

But $L(s) \cup (IUTUR)(s) = N(s) = N(LP(s)) \cup N(RP(s)$, and $L(s) \cap (IUTUR)(s) = \emptyset$.

Hence $L(s) = N(LP(s))$ and $(IUTUR)(s) = N(RP(s))$. #

<u>4.29 LEMMA</u> Let $s.s = s \in \mathcal{S}(J)$.

Then $LP(s).LP(s) = LP(s)$ and $RP(s).RP(s) = RP(s)$ in $\mathcal{S}(J)$, and $H_s | H_{LP(s)} \times H_{RP(s)}$.

<u>Proof</u> : (i) Let $g,h \in H_s$.

Then $g.h = LP(g).LP(h) \cup LP(g).RP(h) \cup RP(g).LP(h) \cup RP(g).LP(h)$.

We have $LP(g).LP(h) = L(s).g.L(s).L(s).h.L(s)$

$$\subseteq L(s).g.s.h.L(s) = L(s).g.h.L(s) = LP(g.h)$$

Also $RP(g).RP(h) = (IUTUR)(s).g.(IUTUR)(s)^2.h.(IUTUR)(s)$

$$\subseteq (IUTUR)(s).g.s.h.(IUTUR)(s) = RP(g.h).$$

Using (4.25 (ii)) we find $LP(g).RP(h) = RP(g).LP(h) = \emptyset$.

Thus $g.h = LP(g).LP(h) \cup RP(g).RP(h)$

$\subseteq LP(g.h) \cup RP(g.h)$

$= g.h.$

Then $LP(g).LP(h) = LP(g.h)$ and $RP(g).RP(h) = RP(g.h)$, since $LP(g.h) \cap RP(g.h) = \emptyset$.

Substituting s for g and h we obtain the first part of the lemma.

Certainly $LP(s), RP(s) \varepsilon S(J)$ since they are subsets of s.

(ii) We have $LP(g).LP(g^{-1}) = LP(s) = LP(g^{-1}).LP(g)$, and $LP(g).LP(s) = LP(g) = LP(s).LP(g)$ for all $g \varepsilon H_s$.

Thus $LP(g) \varepsilon H_{LP(s)}$ for all $g \varepsilon H_s$.

Similarly it can be shown that $RP(g) \varepsilon H_{RP(s)}$ for all $g \varepsilon H_s$.

(iii) The map $\psi : H_s \to H_{LP(s)} \times H_{RP(s)}$ defined by :

$\psi : g \mapsto [LP(g),RP(g)]$ for all $g \varepsilon H_s$, is a monomorphism (from (i) and (ii)). Thus $H_s | H_{LP(s)} \times H_{RP(s)}$. #

4.30 DEFINITION Let $s.s = s \varepsilon S(J)$. Let $g \varepsilon H_s$.

Define

(i) $IP(g) = (IUR)(s).g.(IUR)(s)$

(ii) $TP(g) = T(s).g.T(s)$

(iii) $YP(g) = (IUR)(s).g.T(s)$.

Notice that these are disjoint subsets of g.

4.31 LEMMA Let $s.s = s \varepsilon S(J)$, such that $L(s) = \emptyset$.

Then

(i) $g = IP(g) \cup YP(g) \cup TP(g)$ for all $g \in H_s$

(ii) $IP(g).IP(h) = IP(g.h)$

(iii) $TP(g).TP(h) = TP(g.h)$

(iv) $YP(g.h) = IP(g).YP(h) \cup IP(g).TP(h) \cup YP(g).TP(h)$,

for all $g,h \in H_s$.

Proof : (i) Let $g \in H_s$. We have

$$T(s).g.(I\cup R)(s) = \{(p,x,q) \in DSw_1w_2(g) \mid (w_1,w_2) \in T(s) \times (I\cup R)(s)\}.$$

But $DSw_1w_2(g) = \emptyset$ whenever $w_1 \in T(s)$, $w_2 \notin T(s)$.

Thus $T(s).g.(I\cup R)(s) = \emptyset$.

Now
$$g = N(s).g.N(s) = [(I\cup R)(s) \cup T(s)].g.[(I\cup R)(s) \cup T(s)] = IP(g) \cup YP(g) \cup TP(g).$$

Notice also that

$$T(s).(I\cup R)(s) \subseteq T(s).T(s).(I\cup R)(s) \subseteq T(s).s.(I\cup R)(s) = \emptyset.$$

(ii) Let $g,h \in H_s$.

Then
$$IP(g).IP(h) = (I\cup R)(s).g.(I\cup R)(s)^2.h.(I\cup R)(s) \subseteq (I\cup R)(s).g.s.h.(I\cup R)(s) = IP(g.h).$$

Also

$$TP(g).TP(h) = T(s).g.T(s)^2.h.T(s) \subseteq T(s).g.s.h.T(s) = TP(g.h).$$

Further
$$IP(g).TP(h) = (I\cup R)(s).g.(I\cup R)(s).T(s).h.T(s) \subseteq (I\cup R)(s).g.s.s.h.T(s) = YP(g.h).$$

Similarly $IP(g).YP(h) \subseteq YP(g.h)$, and $YP(g).TP(h) \subseteq YP(g.h)$.

However $YP(g).IP(h) = (I\cup R)(s).g.T(s).(I\cup R)(s).h.(I\cup R)(s) = \emptyset$,

and similarly we show $YP(g).YP(h) = TP(g).IP(h) = TP(g).YP(h) = \emptyset$.

Thus

$$g.h = IP(g).IP(h) \cup TP(g).TP(h) \cup [IP(g).YP(h) \cup IP(g).TP(h) \cup YP(g).TP(h)]$$
$$\subseteq IP(g.h) \cup TP(g.h) \cup YP(g.h)$$
$$= g.h.$$

From this we see that $IP(g).IP(h) = IP(g.h)$,

$$TP(g).TP(h) = TP(g.h)$$

and $IP(g).YP(h) \cup IP(g).TP(h) \cup YP(g).TP(h) = YP(g.h)$. #

4.32 LEMMA Let $s.s = s \in S(J)$. Let $L(s) = \emptyset$.

Then $IP(s).IP(s) = IP(s)$, $TP(s).TP(s) = TP(s)$,

and $H_s | H_{IP(s)} \times H_{TP(s)}$.

Proof : The first part follows immediately from the previous theorem, by substituting $s = g = h$ in (ii) and (iii).

It also follows that for all $g \in H_s$, $IP(g) \in H_{IP(s)}$ and $TP(g) \in H_{TP(s)}$.

Now $YP(g) = IP(g).YP(s) \cup IP(g).TP(s) \cup YP(g).TP(s)$ for all $g \in H_s$.

But $TP(s) = TP(g^{-1}).TP(g)$ so that

$YP(g).TP(s) = YP(g).TP(g^{-1}).TP(g) \subseteq YP(s).TP(g)$.

Thus $YP(g) \subseteq IP(g).YP(s) \cup IP(g).TP(s) \cup YP(s).TP(g) \subseteq YP(g)$.

and $g = IP(g) \cup TP(g) \cup IP(g).YP(s) \cup IP(g).TP(s) \cup YP(s).TP(g)$. (*)

Hence the map $\psi : H_s \to H_{IP(s)} \times H_{TP(s)}$ defined by :

$$\psi : g \mapsto [IP(g),TP(g)] \quad \text{for all } g \in H_s,$$

is a monomorphism, (3.31) and (*).

Thus $H_s | H_{IP(s)} \times H_{TP(s)}$. #

4.33 LEMMA Let $s.s = s \in S(J)$.

Then

(i) $L(LP(s)) = N(LP(s)) = L(s)$, $LP(s) = N(LP(s)).LP(s).N(LP(s))$

(ii) $L(TP(s)) = N(TP(s)) = T(s)$, $TP(s) = N(TP(s)).TP(s).N(TP(s))$

(iii) $IP(s) \in \mathcal{S}(J)$, and satisfies the conditions of (4.5) and (4.13).

Proof : (i) Certainly $L(LP(s)) \subseteq N(LP(s))$.

Now
$$\begin{aligned} LP(s) = L(s).s.L(s) &= \{(p,x,q) \in DSww'(s) \mid (w,w') \in L(s)\times L(s)\} \\ &= \{(p,x,q) \in DSww(s) \mid w \in L(s)\} \\ &= \{(p,x,q) \in w(s) \mid w \in L(s)\}. \end{aligned}$$

Suppose $(p,y,p) \in N(LP(s))$. Then $(p,y,p) \in w(s)$ for some $w \in L(s)$, where $w = (p,x,p)$. But $y^2 = y$ and $x^2 = x$ and $x \mathcal{H} y$ implies $x = y$. Thus $(p,y,p) \in L(s)$ and $N(LP(s)) \subseteq L(s)$. Now $DSww'(LP(s)) \subseteq DSww'(s)$ for all $(w,w') \in N(s) \times N(s)$. Thus $DSww'(LP(s)) = \emptyset$ for all $w,w' \in N(LP(s)) \subseteq L(s)$ whenever $w \neq w'$. Thus $N(LP(s)) \subseteq L(LP(s))$, and $N(LP(s)) = L(LP(s))$.

Also $L(s) \subseteq L(s)^3 \subseteq L(s).s.L(s) = LP(s)$ and $w \in L(s) \Rightarrow w = (q,x,q)$ where $x^2 = x$. Thus $w \in N(LP(s))$. Hence $L(s) \subseteq N(LP(s))$, and $L(s) = N(LP(s))$.

Further
$$\begin{aligned} LP(s) = L(s).s.L(s) &\subseteq L(s)^2.s.L(s)^2 \subseteq N(LP(s)).L(s).s.L(s).N(LP(s)) \\ &= N(LP(s)).LP(s).N(LP(s)) \subseteq LP(s)^3 = LP(s). \end{aligned}$$

Thus $LP(s) = N(LP(s)).LP(s).N(LP(s))$.

(ii) We have $L(TP(s)) \subseteq N(TP(s))$.

Now
$$TP(s) = T(s).s.T(s) = \{(p,x,q) \in DSww'(s) \mid (w,w') \in T(s) \times T(s)\}$$

But $DSww'(s) = \emptyset$ whenever $w \in T(s)$ and $w' \neq w$ for $w' \in N(s)$.

Thus $TP(s) = \{(p,x,q) \in DSww(s) | w \in T(s)\}$

$= \{(p,x,q) \in w(s) | w \in T(s)\}$.

In exactly the same way as in part (i) we can show that $N(TP(s)) \subseteq T(s)$, and that for $w \in N(TP(s))$, $DSww'(TP(s)) = \emptyset$, when $w \neq w'$. Suppose $w' \in N(TP(s))$ and $DSw'w(TP(s)) \neq \emptyset$. Then $w' \in T(s)$ implies $w' = w$. Thus $N(TP(s)) \subseteq L(TP(s))$.

The remainder of the proof is similar to that of part (i), replacing $L(s)$ by $T(s)$ and $LP(s)$ by $TP(s)$.

(iii) Certainly $IP(s) \in S(J)$, since $IP(s) \subseteq s \in S(J)$.

Now $IP(s) = (IUR)(s).s.(IUR)(s)$.

Suppose $w \in (IUR)(s)$. Then $w = w^3 \in (IUR)(s).s.(IUR)(s)$. Hence $w \in N(IP(s))$, and $(IUR)(s) \subseteq N(IP(s))$. We have $(IUR)(s).(IUR)(s) \subseteq (IUR)(s)$, since $(IUR)(s) \subseteq N(s)$. Thus

$$\begin{aligned} IP(s) &\subseteq (IUR)(s)^2.s.(IUR)(s^2) \\ &\subseteq N(IP(s)).(IUR)(s).s.(IUR)(s).N(IP(s)) \\ &= N(IP(s)).IP(s).N(IP(s)) \\ &\subseteq IP(s).IP(s).IP(s) \\ &= IP(s). \end{aligned}$$

Hence $IP(s) = N(IP(s)).IP(s).N(IP(s))$.

Thus $IP(s)$ satisfies condition (4.5).

That $IP(s)$ satisfies the conditions of (4.13) follows from its being a subset of s. #

4.34 DEFINITION Let $s.s = s \in S(J)$. Let $(w,w') \in L(s) \times L(s) \cup I(s) \times T(s)$, with $DSww'(s) \neq \emptyset$.

Define a set $P_{ww'} = \{w,w_1,\ldots,w_k,w'\} \subseteq N(s)$ to be a path from w to w' in s if

(i) $w_i = w_j$ iff $i = j$ for $1 \leq i \leq j \leq k$,

(ii) $w \neq w_i$, $w_i \neq w'$ for $1 \leq i \leq k$,

and (iii) $DSww_1(s) \neq \emptyset$, $DSw_iw_{i+1}(s) \neq \emptyset$, $DSw_kw'(s) \neq \emptyset$ for $1 \leq i \leq k - 1$.

Define the <u>length of the path</u> $P_{ww'}$ to be $|P_{ww'}| - 1$.

[Recall that $DSvv'(s) \neq \emptyset$ implies $DSv'v(s) = \emptyset$ for all $v,v' \in N(s)$].

We see that if $w \in L(s)$, then $DSww'(s) \neq \emptyset$ implies $w = w'$ and the only path from w to w is $\{w\}$. We have defined the length of this path to be zero.

It is obvious that there are no paths from w to w' when $(w,w') \in L(s) \times T(s) \cup I(s) \times L(s)$.

Define $k_{ww'}(s)$ to be the maximum of the lengths of all paths from w to w' in s. Certainly $k_{ww'}(s)$ is finite.

Define $k(s) = \max \{k_{ww'}(s) \mid (w,w') \in L(s) \times L(s) \cup I(s) \times T(s)\}$.

<u>4.35 LEMMA</u> Let $s \circ s = s \in \mathcal{S}(J)$.

Then (i) $LP(s) \neq \emptyset$ implies $k(LP(s)) = 0$.

(ii) $RP(s) \neq \emptyset$ implies $k(RP(s)) = k(s)$

(iii) $k(IP(s)) = k(RP(s)) - 1$, when $RP(s) \neq \emptyset$

(iv) $k(s) = 0$ implies $L(s) = N(s)$.

<u>Proof</u> : (i) Let $LP(s) \neq \emptyset$. We have $N(LP(s)) = L(LP(s))$. Thus $(w,w') \in L(LP(s)) \times L(LP(s)) \cup I(LP(s)) \times T(LP(s))$ implies $(w,w') \in L(LP(s)) \times L(LP(s))$. We saw that any path from w to w' must be from w to itself, and have zero length. Thus $k(LP(s)) = 0$.

(ii) Let $RP(s) = \emptyset$. Let $k(RP(s)) = \ell$. Let $(w,w') \in I(s) \times T(s)$, such that there exists $P_{ww'} \subseteq N(RP(s))$ with length ℓ. We have $N(RP(s)) = (I \cup T \cup R)(s)$, so that $P_{ww'} \subseteq (I \cup T \cup R)(s) \subseteq N(s)$, and $P_{ww'}$ satisfies the requirements of a path from w to w' in s. Thus $k(RP(s)) \leq k(s)$.

Conversely, if $P_{ww'}$ is a path in s, where $(w,w') \in I(s) \times T(s)$, then $P_{ww'} \subseteq (I \cup T \cup R)(s) = N(RP(s))$. Thus $P_{ww'}$ is a path in $RP(s)$. Hence $k(s) \leq k(RP(s))$.

(iii) Let $(w,w') \in L(IP(s)) \times L(IP(s)) \cup I(IP(s)) \times T(IP(s))$ such that there exists a path $P_{ww'} \subseteq N(IP(s))$ of length $k(IP(s))$. We have $DSw'w''(IP(s)) = \emptyset$ whenever $w'' \neq w'$. Thus there exists $w'' \in TP(s)$ such that $DSw'w''(RP(s)) \neq \emptyset$, otherwise $w' \in TP(s)$ and $w' \notin IP(s)$. Now $P_{ww'} \cup \{w''\}$ is a path from w to w'' in $RP(s)$ of length $k(IP(s)) + 1$. Thus $k(RP(s)) \geq k(IP(s)) + 1$.

Conversely, let $(w,w') \in I(RP(s)) \times T(RP(s))$ and $P_{ww'}$ be a path of length $k(RP(s))$. Suppose $P_{ww'} = \{w,w_1,\ldots,w_\ell,w'\}$. Suppose $DSw_\ell w''(IP(s)) \neq \emptyset$. Then there exists $w''' \in TP(s)$ such that $DSw''w'''(RP(s)) \neq \emptyset$ and a path $P_{ww'''} \subseteq N(RP(s))$ of length $k(RP(s)) + 1$. Thus $DSw_\ell w''(IP(s)) \neq \emptyset$ implies $w'' = w_\ell$, that is $w'' \in L(IP(s)) \cup T(IP(s))$. Now $P_{ww_\ell} \subseteq N(IP(s))$ is a path from w to w_ℓ in $IP(s)$ of length $k(RP(s)) - 1$, for $IP(s) \subseteq RP(s)$ implies $(I \cup L)(IP(s)) \subseteq I(RP(s))$. Thus $k(IP(s)) \geq k(RP(s)) - 1$.

Hence $k(RP(s)) = k(IP(s)) + 1$.

(iv) Suppose $k(s) = 0$ and $RP(s) \neq \emptyset$. Then there exists $(w,w') \in I(s) \times T(s)$ such that $P_{ww'}$ is a path of length at least 1. Thus $k(s) \geq 1$. Hence $RP(s) = \emptyset$, so that $(I \cup T \cup R)(s) = \emptyset$ and $N(s) = L(s)$. #

4.36 THEOREM Let $s.s = s \in S(J)$.

Then

$$H_s \mid \prod_{i=1}^{m} H_{s_i},$$

where $N(s_i) = L(s_i)$ for $1 \leq i \leq m$ and $m \leq 2k(s) + 1$.

Proof : For any such $s \in S(J)$ we have

$$H_s | H_{LP(s)} \times H_{RP(s)}, \quad H_{RP(s)} | H_{IP(s)} \times H_{TP(s)} \quad \text{and that}$$

$$L(LP(s)) = N(LP(s)) \quad \text{and} \quad L(TP(s)) = N(TP(s)).$$

Put $s_{11} = LP(s)$, $s_{12} = TP(s)$ and $s_{13} = IP(s)$.

Then $H_s | H_{s_{11}} \times H_{s_{12}} \times H_{s_{13}}$,

where $s_{13}.s_{13} = s_{13} \in S(J)$ satisfying the conditions of (4.5) and (4.13), and $k(s_{13}) = k(s) - 1$.

Now for $1 \leq i \leq k(s) - 1$ put
$$s_{i+1,1} = LP(s_{i3})$$
$$s_{i+1,2} = TP(s_{i3})$$
$$s_{i+1,3} = IP(s_{i3}).$$

We have $L(s_{i1}) = N(s_{i1})$, $L(s_{i2}) = N(s_{i2})$, $s_{i3}.s_{i3} = s_{i3} \in S(J)$, $k(s_{i3}) = k(s_{i-1,3}) - 1 = k(s) - i$, and s_{i3} satisfies (4.5) and (4.13), for $1 \leq i \leq k(s)$. Further we have $k(s_{k(s),3}) = 0$, so that $L(s_{k(s),3}) = N(s_{k(s),3})$.

Using transitivity of division of semigroups and the fact that

$$H_{s_{i3}} | H_{s_{i+1,1}} \times H_{s_{i+1,2}} \times H_{s_{i+1,3}} \quad \text{for } 1 \leq i \leq k(s) - 1,$$

we find $H_s \mid \prod_{i=1}^{k(s)} (H_{s_{i1}} \times H_{s_{i2}}) \times H_{s_{k(s),3}}$.

Some of the s_{i1} may be void for $1 \leq i \leq k(s)$, so the groups $H_{s_{i1}}$ attached to these can be taken to be groups of order 1, and have no effect on the product.

Thus $H_s \mid \prod_{i=1}^{m} H_{s_i}$ where $m \leq 2k(s) + 1$ and $N(s_i) = L(s_i)$ for $1 \leq i \leq n$.

4.37 REMARK It can be seen that the s_i of the previous theorem satisfy the conditions :

(i) $s_i = N(s_i).s_i.N(s_i)$

and (ii) $N(s_i) = L(s_i)$.

The latter condition implies that the s_i also satisfy the conditions 4.13 (i) & (ii), since $Dw(s_i) = Sw(s_i) = \emptyset$ for all $w \in N(s_i) = L(s_i)$.

CHAPTER 5. THE SIMPLE GROUPS WHICH DIVIDE $S(M)$.

5.1 REMARK Suppose s is an idempotent of a semigroup $S(J)$, where J is a J class of $S(M)$, and $s = N(s).s.N(s)$ and $N(s) = L(s)$. We show that H_s divides a direct product of groups associated with idempotents, t, of $S(J)$, with the properties $t = N(t).t.N(t)$ and $t = L(t)$. It is then shown that a group H_t, where t is such an idempotent, divides a semidirect product $(\prod_{i=1}^{n} H_{y_i}) \times_\phi P_n$, when the y_i are idempotents of J, and P_n is the permutation group on n characters, where $n = |t|$.

The result is further refined by showing that H_t divides a direct product of groups of type $H_{t'}$, when $t = L(t) = N(t).t.N(t)$, and where $t'.t' = t' \varepsilon S(J)$ such that for any $w,w' \varepsilon N(t') = L(t') = t' = N(t').t'.N(t')$ there exists $(p,x,q) \varepsilon T(M)$ such that $x \varepsilon J$ and $w.(p,x,q).w' = (p,x,q)$.

Hence any simple group dividing $S(M)$ must divide either $Sch(J)$, the Schutzenberger group of the J class J of $S(M)$, or $P_{n(J)}$ where $n(J)$ is the maximum cardinality of the idempotents of $S(J)$ satisfying the conditions of t' above. This is so since $Sch(J) \cong H_y$, whenever y is an idempotent in J. Further it is shown that if G is a group such that $G|Sch(J)$ then $G|P_{n(J)}$. Also that if $G|P_{n(J)}$ then $G|S(M)$.

We conclude that the simple groups dividing $S(M)$ are exactly the simple groups which divide $P_{n(M)}$, where $n(M) = \max\{n(J)|J$ is a J class of $S(M)\}$.

<u>5.2 REMARK</u> Recall (4.15) which states;

Let $s.s = s \in S(J)$ and $w \in N(s)$. Let $g \in H_s$.

Then

(i) $DSww'(g) \neq \emptyset$ for some $w' \in N(s)$,

(ii) $DSw'w(g) \neq \emptyset$ for some $w' \in N(s)$.

All idempotents referred to in this chapter will have the properties $s = N(s).s.N(s)$ and $N(s) = L(s)$.

<u>5.3 LEMMA</u> Let $s.s = s \in S(J)$. Let $g \in H_s$, $w \in N(s)$.

Then

(i) $DSww'(g) \neq \emptyset$ for $w' \in N(s)$ implies $DSww''(g) = \emptyset$ whenever $w' \neq w'' \in N(s)$.

(ii) $DSw'w(g) \neq \emptyset$ for $w' \in N(s)$ implies $DSw''w(g) = \emptyset$ whenever $w' \neq w'' \in N(s)$.

<u>Proof</u> : (i) There exists $w' \in N(s)$ such that $DSww'(g) \neq \emptyset$. Suppose $w_1 \in N(s)$ such that $DSw'w_1(g^{-1}) \neq \emptyset$. Then $DSww_1(s) \neq \emptyset$, and $w = w_1$ since $N(s) = L(s)$. Suppose $w'' \in N(s)$ and $DSww''(g) \neq \emptyset$. Then

$DSw'w''(s) \supseteq DSw'w(g^{-1}).DSww''(g) \neq \emptyset$. Hence $w'' = w'$, and we have the result.

(ii) This is the dual of part (i). #

<u>5.4 REMARK</u> We see from the previous lemmas that for each $g \in H_s$, we may associate a unique permutation, $P(g)$, on the set $N(s)$ defined by

$P(g) : w \mapsto w'$ iff $DSww'(g) \neq \emptyset$; for all $w \in N(s)$.

The mapping is well defined and 1:1, from (5.3).

5.5 LEMMA Let $s.s = s \in \mathcal{S}(J)$. Let $g,h \in H_s$.

Then for $w,w_1,w_2,w_3 \in N(s)$ such that $DSww_1(g) \neq \emptyset$ and $DSw_2w_3(h) \neq \emptyset$, we have $DSww_3(g.h) \neq \emptyset$ iff $w_1 = w_2$.

Also $(p,x,q).(q,y,r) \neq \emptyset$ whenever $w_1 = w_2$ and $[(p,x,q),(q,y,r)] \in DSww_1(g) \times DSw_2w_3(h)$.

Proof : $DSww_1(g).DSw_2w_3(h) = w.g.w_1.w_2.h.w_3 \neq \emptyset$ implies $w_1.w_2 \neq \emptyset$. Thus $w_1.w_2 \in DSw_1w_2(s)$. But $DSw_1w_2(s) \neq \emptyset$ implies $w_1 = w_2$. Notice that w_1,w_2 are unique from (5.3). ~~The converse follows.~~ The converse follows from (4.15).

The second part of the statement is proved in (4.15 (ii)). #

5.6 LEMMA Let $s.s = s \in \mathcal{S}(J)$, with $s = L(s)$.

Then

(i) $|g| = |s|$ for all $g \in H_s$

(ii) $|g.h| = |g| = |h|$ for all $g,h \in H_s$

(iii) If O_1, O_2 are distinct orbits of P_g where $g \in H_s$, then $g_{O_1}.g_{O_2} = \emptyset$, where $g_{O_i} = O_i.g.O_i$ for $i = 1,2$, and we consider the O_i as subsets of $N(s)$, and thus as elements of $\mathcal{S}(J)$.

Proof : (i) Put $N(s) = \{w_1,\ldots,w_k\}$. Let $g \in H_s$. Define a permutation P_g on $\{1,\ldots,k\}$ by $P_g : i \to j$ iff $DSw_iw_j(g) \neq \emptyset$, for $1 \le i \le k$.

From (5.3) we have $g = \{(p,x,q) \in DSw_iw_{P_g(i)}(g) | w_i \in N(s)\}$,

Now $DSw_iw_{P_g(i)}(g).(p,x,q) \neq \emptyset$, where $(p,x,q) \in DSw_{P_g(i)}w_i(g^{-1})$.

[$DSw_{P_g(i)}w_i(g^{-1}) \neq \emptyset$, since there must exist $w' \in N(s)$ such that $DSw_{P_g(i)}w'(g^{-1}) \neq \emptyset$, and thus $DSw_iw'(s) \neq \emptyset$. Hence $w' = w_i$.]

Suppose (q,x_1,p), $(q,x_2,p) \in DSw_i w_{P_g(i)}(g)$. Then $(q,x_1x,q) = (q,x_2x,q) = w_i$; since $s = N(s)$, and $w = w(s)$ for all $w \in N(s)$. Also $(p,xx_1,p) = (p,xx_2,p) = w_{P_g(i)}$. Thus $(q,x_1xx_2,p) = (q,x_1,p).w_{P_g(i)} = (q,x_1,p)$. Also $(q,x_1xx_2,p) = w_i.(q,x_2,p) = (q,x_2,p)$. Thus $(q,x_1,p) = (q,x_2,p)$ and $|DSw_i w_{P_g(i)}(g)| = 1$, for all $w_i \in N(s)$.

Now $g = \{\bigcup_{i=1}^{k} DSw_i w_{P_g(i)}(g)\}$ so that $|g| = |N(s)| = |s|$.

(ii) This follows immediately from part (i).

(iii) $g_{O_1}.g_{O_2} = O_1.g.O_1.O_2.g.O_2$. Now $s = L(s)$ implies $w_1.w_2 = 0$ whenever $w_1,w_2 \in N(s)$ and $w_1 \neq w_2$. Now $O_1 \cap O_2 = \emptyset$ since they are distinct orbits of $P(g)$. Thus $O_1.O_2 = \{w_1.w_2 | w_1 \in O_1, w_2 \in O_2\} = \emptyset$. Hence $g_{O_1}.g_{O_2} \neq \emptyset$. #

5.7 LEMMA Let $s.s = s \in S(J)$.

Then

$$H_s | H_{N(s)}.$$

Proof : (i) We have
$L(s).L(s) = \{w_1.w_2 \mid w_1, w_2 \in L(s)\} = \{w^2 | w \in L(s)\} = L(s)$, since $w_1.w_2 \in DSw_1w_2(s) = \emptyset$ whenever $w_1 \neq w_2$. Thus $N(s).N(s) = N(s)$. Similarly we may show $N'.N' = N'$ for any $N' \subseteq L(s)$.

Let $g \in H_s$. Let $O_1,\ldots,O_k$ be the orbits of $P(g)$.

Put $O_i = \{w_{i1},\ldots,w_{i\ell_i}\}$ where $\ell_i = |O_i|$, and

$DSw_{ij}w_{i,j+1}(g) \neq \emptyset$ for $1 \leq j \leq \ell_i$, $1 \leq i \leq k$. [We shall assume $p_{i,\ell_i+1} = p_{i1}$ and $w_{i,\ell_i+1} = w_{i1}$ for $1 \leq i \leq k$, throughout this proof.]

Put $w_{ij} = (p_{ij}, z_{ij}, p_{ij})$ for $1 \le j \le \ell_i$, $1 \le i \le k$.

Let $t_i = \{(p_{i1}, x_{i1}, p_{i2}), \ldots, (p_{i\ell_i}, x_{i\ell_i}, p_{i1})\}$ be a subset of $\bigcup_{j=1}^{\ell_i} DSw_{ij}w_{i,j+1}(g)$, such that $|t_i \cap DSw_{ij}w_{i,j+1}(g)| = 1$ for $1 \le j \le \ell_i$, and where $(p_{ij}, x_{ij}, p_{i,j+1}) = t_i \cap DSw_{ij}w_{i,j+1}(g)$ for $1 \le j \le \ell_i$. Thus $|t_i| = \ell_i$.

Now

$$O_i.t_i = \{(p_{im}, z_{im}, p_{im}).(p_{ij}, x_{ij}, p_{ij}) \in DSw_{im}w_{im}(s).DSw_{ij}w_{i,j+1}(s) \mid 1 \le m \le \ell_i \text{ and } 1 \le j \le \ell_i\}.$$

Using lemma 5.5 we see that :

$$\begin{aligned} O_i.t_i &= \{w_{im}.(p_{im}, x_{im}, p_{i,m+1}) \mid 1 \le m \le \ell_i\} \\ &= \{(p_{im}, x_{im}, p_{i,m+1}) \mid 1 \le m \le \ell_i\} \\ &= t_i . \end{aligned}$$

Dually $t_i.O_i = t_i$.

Again using lemma 5.5, and recalling that the w_{ij} are distinct, it can be seen that for $r \in Z^+$:

$$(t_i)^r \in \bigcup_{j=1}^{\ell_i} DSw_{ij}w_{i,f_j(r)}(g^r) \quad \text{where} \quad f_j(r) = (j+r)(\text{mod } \ell_i),$$

for $1 \le j \le \ell_i$. Further we have :

$$(t_i)^r \cap DSw_{ij}w_{i,f_j(r)}(g^r) = \prod_{k=0}^{r-1} [t_i \cap DSw_{i,f_j(k)}w_{i,f_j(k)+1}(g)],$$

and since the cardinality of all the factors in the product is 1, we must have $|(t_i)^r \cap DSw_{ij}w_{i,f_j(r)}(g^r)| = 1$, and $|(t_i)^r| = |t_i| = \ell_i$, for $r \in Z^+$, and $1 \le i \le \ell_i$.

Now $\prod_{j=1}^{\ell_i} x_{ij} \mathcal{J} z_{i1}$, since $(p_{i1}, \prod_{j=1}^{\ell_i} x_{ij}, p_{i1}) \ne \emptyset$. In fact $\prod_{j=1}^{\ell_i} x_{ij} \mathcal{H} z_{i1}$, since $x_{i1} \mathcal{R} z_{i1} \mathcal{L} x_{i\ell_i}$. Since $H_{z_{i_1}}$ is a subgroup of $S(M)$ there exists $k(t_i) \in Z^+$ such that

$$(\prod_{j=1}^{\ell_i} x_{ij})^{k(t_i)} = z_{i1}.$$

From (3.7) and the fact that $z_{i1}x_{i1} = x_{i1}$, we have

$$(\prod_{j=m}^{\ell_i} x_{ij}).(\prod_{j=1}^{\ell_i} x_{ij})^{k(t_i)-1}(\prod_{i=1}^{m-1} x_{ij}) = z'_{im}, \text{ where } (z'_{im})^2 = z'_{im},$$

for $2 \le m \le \ell_i$.

Further $z'_{im} \mathcal{R} x_{im} \mathcal{R} z_{im}$ and $z'_{im} \mathcal{L} x_{i,m-1} \mathcal{L} z_{im}$. Thus $z'_{im} \mathcal{H} z_{im}$, and since they are both idempotents of $S(M)$ we have $z'_{im} = z_{im}$ for $2 \le m \le \ell_i$.

We see therefore that $(p_{im}, z_{im}, p_{im}) \in (t_i)^{\ell_i k(t)}$ for $1 \le m \le \ell_i$. That is $O_i \subseteq (t_i)^{\ell_i k(t_i)}$. But $|(t_i)^{\ell_i k(t_i)}| = \ell_i = |O_i|$. Hence $O_i = (t_i)^{\ell_i k(t_i)}$.

From this and $t_i.O_i = t_i = O_i.t_i$, we have $t_i \in H_{O_i}$. Certainly $O_i.O_i = O_i$, since $O_i \subseteq L(s)$.

Let $t_i \subseteq \bigcup_{j=1}^{\ell_i} DSw_{ij}w_{i,j+1}(g)$, for $1 \le i \le k$, be subsets of the type considered above.

Let $t = \bigcup_{i=1}^{k} t_i$. Let $n = \mathrm{LCM}\,\{\ell_i k(t_i) \mid 1 \leq i \leq k\}$.

Then $t^n = \bigcup_{i=1}^{k} (t_i)^n$, since $t_i = O_i.t_i.O_i \subseteq g_{O_i}$ for $1 \leq i \leq k$, and $t_i.t_j \subseteq g_{O_i}.g_{O_j} \neq \emptyset$ whenever $i \neq j$.

Thus $t^n = \bigcup_{i=1}^{k} (O_i)^{n/\ell_i k(t_i)} = \bigcup_{i=1}^{k} O_i = N(s)$

Also $t.N(s) = (\bigcup_{i=1}^{k} t_i).(\bigcup_{i=1}^{k} O_i) = \bigcup_{i=1}^{k} t_i.O_i$, since $O_i = O_i^3 \subseteq g_{O_i}$ for $1 \leq i \leq k$. Thus $t.N(s) = \bigcup_{i=1}^{k} t_i = t$.

Dually $t = N(s).t$.

Put $F(g) = \{t \subseteq g \mid |t \cap DSww'(g)| = 1$, whenever $DSww'(g) \neq \emptyset$ for $w,w' \in N(s)\}$.

We have shown that any $t \in F(g)$ is an element of $H_{N(s)}$. Thus $F(g) \subseteq H_{N(s)}$.

(ii) Let $t \in F(g)$, for $g \in H_s$, such that $g^m = s$. Let $t^n = N(s)$. Then

$g = s.g = s.N(s).g = s.t.t^{mn-1}.g \subseteq s.t.g^{mn-1}.g = s.t.s \subseteq s.g.s = g$.

Thus $g = s.t.s$ for any $t \in F(g)$, for all $g \in H_s$.

Further for $g,h \in H_s$, $F(g) \cap F(h) \neq \emptyset$ iff $g = h$.

(iii) Let $t_g \in F(g)$, $t_h \in F(h)$ where $g,h \in H_s$.

From (5.6) we have $|t_g| = |t_h| = |t_g.t_h| = |N(s)|$.

Put $N(s) = \{w_1,\ldots,w_m\}$ where $m = |N(s)|$.

For $g \in H_s$, define a permutation P_g on $\{1,\ldots,m\}$ by

$$P_g : i \mapsto j \text{ iff } DSw_iw_j(g) \neq \emptyset .$$

Using (5.3) and (5.5) we see that

$$DSw_i w_{P_g(i)}(g).DSw_{P_g(i)} w_{P_h(P_g(i))}(h) \subseteq DSw_i w_{P_{g.h}(i)}(g.h), \quad \text{for } 1 \le i \le m.$$

Thus $t_g.t_h \cap DSw_i w_{P_{g.h}(i)}(g.h) \supseteq$

$$[t_g \cap DSw_i w_{P_g(i)}(g)].[t_h \cap DSw_{P_g(i)} w_{P_h(P_g(i))}(h)].$$

Hence $|t_g.t_h \cap DSw_i w_{P_{g.h}(i)}(g.h)| \ge 1$, for $1 \le i \le m$, since each factor in the products has cardinality 1. Combining this result with the fact that $|t_g.t_h| = m$, we must have

$$|t_g.t_h \cap DSw_i w_{P_{g.h}(i)}(g.h)| = 1 \quad \text{for } 1 \le i \le m.$$

Thus $t_g.t_h \in F(g.h)$, and $F(g).F(h) \subseteq F(g.h)$.

Let $\mathcal{F} = \bigcup_{g \in H_s} F(g) \subseteq H_{N(s)}$. Then $\mathcal{F}$ is a subsemigroup of $H_{N(s)}$.

(iv) Define a map $\psi : \mathcal{F} \to H_s$ by :

$$\psi : t \mapsto g \text{ iff } t \in F(g), \text{ for all } t \in \mathcal{F}.$$

From (ii) we know the map is well defined, and from (iii) we know that it is a homomorphism.

Thus $H_s | H_{N(s)}$. #

<u>5.8 THEOREM</u> Let $s.s = s \in S(J)$. Let $s = N(s) = L(s)$.

Suppose $s = \{w_1, \ldots, w_n\}$ and $w_i = (q_i, y_i, q_i)$ for $1 \le i \le n$.

Then $H_s | (H_{y_1} \times \ldots \times H_{y_n}) \times_\phi P_n$, where ϕ is an homomorphism from P_n into $\mathrm{Endo}_L(\prod_{i=1}^{n} H_{y_i})$, and P_n is the permutation group on n characters.

<u>Proof</u> : (i) Suppose $g \in H_s$. Then $g = \{(q_i, y_{iP_g(i)}, q_{P_g(i)}) \mid 1 \leq i \leq n\}$. Here P_g is the permutation on $\{1,\ldots,n\}$ defined by :

$$P_g : i \mapsto j \quad \text{iff} \quad DSw_i w_j(g) \neq \emptyset .$$

We define the semigroup J^0 to be the set $J \cup \{0\}$ with multiplication defined by $xy = \begin{cases} xy, & \text{when } xy \in J \\ 0, & \text{otherwise.} \end{cases}$

We construct a partial representation of this semigroup as follows (after [REES]) :

Let $\{x_1,\ldots,x_m\} = \{y_1,\ldots,y_n\}$ with $x_i = x_j$ iff $i = j$. [The y_i may not be distinct.]

Define a map $a : \{1,\ldots,n\} \to \{1,\ldots,m\}$ by $a : i \mapsto j$ iff $y_i = x_j$.

Put $H_{11} = H_{x_1}$. Let $r_1 = \ell_1 = x_1$.

Select $\ell_i \in L_{x_1} \cap R_{x_i}$, $r_i \in R_{x_1} \cap L_{x_i}$ such that $r_i \ell_i = x_i$.

This is possible, since given $\ell_i \in L_{x_1} \cap R_{x_i}$, we have $\ell_i x_1 = \ell_i$, and $x_1 r = r$ for all $r \in R_{x_1} \cap L_{x_i}$. Then $\alpha : H_{11} \to H_{ii}$ defined by $\alpha : t \mapsto \ell_i t r$ for all $t \in H_{x_i}$, where $r \in R_{x_1} \cap L_{x_i}$, is $1 : 1$ and onto. Thus there exists $t \in H_{x_i}$

such that $\ell_i tr = x_i$. But $tr \in R_{x_1} \cap L_{x_i}$, so by putting $tr = r_i$, we find $\ell_i r_i = x_i$, for $1 \leq i \leq m$.

Further since $\ell_i r_i = x_i$, we have $\ell_i (r_i \ell_i)^k r_i = x_i^{k+1} = x_i$ for all $k \in Z^+$. Now $(r_i \ell_i)^k \,H\, x_1$ for all $k \in Z^+$. Thus the map $\beta : H_{x_1} \to H_{x_i}$ defined by $\beta : t \mapsto \ell_i tr_i$ is 1:1. Thus $\ell_i(r_i\ell_i)r_i = \ell_i(r_i\ell_i)^2 r_i$ implies $r_i\ell_i = (r_i\ell_i)^2$. Thus $r_i\ell_i$ is an idempotent in H_{x_1}. Hence $r_i\ell_i = x_1$ for $1 \leq i \leq m$.

Put $H_{ij} = L_{x_i} \cap R_{x_j}$, $1 \leq i,j \leq m$.

Put $t_{ij} = \ell_i r_j \in H_{ij}$. Certainly $\ell_i r_j \neq 0$ since $\ell_i \,L\, x_1$ and $r_j \,R\, x_1$ so that $Z(\ell_i)|P(r_j)$, for $1 \leq i,j \leq m$.

Put $t'_{ij} = \ell_{a(i)} r_{a(j)}$, for $1 \leq i,j \leq n$.

[It will become clear that we need only consider the H classes of J which have been defined so far.]

Suppose $y \in H_{ij}$, $1 \leq i,j \leq m$. Then we have a map $\gamma : H_{ii} \to H_{ij}$ defined by $\gamma : g \mapsto x_i g t_{ij}$ for all $g \in H_{ii}$, which is 1:1 and onto. Thus there exists a unique $g_i \in H_{ii}$ such that $x_i g_i t_{ij} = y$. Also $x_i g_i = g_i$, so that $y = g_i t_{ij}$.

We have seen that for all $g \in H_s$,

$$g = \{(q_i, y_{iP_g(i)}, q_{P_g(i)}) \mid 1 \leq i \leq n\}.$$

Now $(q_i, y_{iP_g(i)}, q_{P_g(i)}) \in DSw_i w_{P_g(i)}(g)$ for $1 \leq i \leq n$.

Thus $\ell_{a[i]} \,R\, x_{a[i]} = y_i \,R\, y_{iP_g(i)} \,L\, y_{P_g(i)} = x_{a[P_g(i)]} \,L\, r_{a[P_g(i)]}$, and $y_{iP_g(i)} \mathcal{H} \ell_{a[i]} r_{a[P_g(i)]} \varepsilon H_{a[i],a[P_g(i)]}$.

Consider the map $\psi : H_s \to (H_{y_1} \times \ldots \times H_{y_n}) \times P_n$ defined as follows :

$$\psi : g = \{(q_i, y_{iP_g(i)}, q_{P_g(i)}) \mid 1 \leq i \leq n\} \mapsto (g_1, \ldots, g_n, P_g),$$

where $g_i \varepsilon H_{y_i} = H_{x_{a[i]}}$ and $g_i t'_{iP_g(i)} = y_{iP_g(i)}$ for $1 \leq i \leq n$, for all $g \varepsilon H_s$.

Since P_g and the g_i thus defined are unique for given $g \varepsilon H_s$, we see that the map is well defined.

Further, given $(g_1, \ldots, g_n, p) \varepsilon (\prod_{i=1}^{n} H_{y_i}) \times P_n$ the set $\{(q_i, g_i t'_{ip(i)}, q_{p(i)}) \mid 1 \leq i \leq n\}$ is uniquely determined. Thus ψ is also 1:1.

(ii) Consider the semidirect product $(\prod_{i=1}^{n} H_{y_i}) \times_\phi P_n$, where $\phi : P_n \to \mathrm{Endo}_L(\prod_{i=1}^{n} H_{y_i})$ is defined by :

$$\phi(p) : (g_1, \ldots, g_n) \mapsto \{t'_{ip(i)} g_{p(i)} t'_{p(i)i} \mid 1 \leq i \leq n\}$$

for all $(g_1, \ldots, g_n) \varepsilon \prod_{i=1}^{n} H_{y_i}$, and for all $p \varepsilon P_n$, where the image is an ordered set by considering the first subscript occuring in each term.

We shall show that $\phi(p) \varepsilon \mathrm{Endo}_L(\prod_{i=1}^{n} H_{y_i})$ for all $p \varepsilon P_n$, and then that ϕ is an homomorphism.

(a) We have

$t'_{ip(i)} g_{p(i)} t'_{p(i)i} = \ell_{a(i)} r_{a[p(i)]} g_{p(i)} \ell_{a[p(i)]} r_{a(i)} \mathcal{H} \ell_{a(i)} r_{a(i)}$.

Thus $t'_{ip(i)} g_{p(i)} t'_{p(i)i} \in H_{x_{a(i)}} = H_{y_i}$ for $1 \leq i \leq n$, where p and g are as defined above. Thus the codomain of $\phi(p)$ is certainly $\prod_{i=1}^{n} H_{y_i}$.

(b) Suppose $(g_1,\ldots,g_n) = g$, $(h_1,\ldots,h_n) = h \in \prod_{i=1}^{n} H_{y_i}$.

Let $p \in P_n$.

(Notice $g,h \notin H_s$ in this section).

Then $\phi(p)(gh) = \{t'_{ip(i)}(gh)_{p(i)}t'_{p(i)i} \mid 1 \leq i \leq n\}$

$= \{t'_{ip(i)}g_{p(i)}h_{p(i)}t'_{p(i)i} \mid 1 \leq i \leq n\}$ since $\prod_{i=1}^{n} H_{y_i}$ is a direct product.

Also $[\phi(p)(g)][\phi(p)(h)]$

$= \{(t'_{ip(i)}g_{p(i)}t'_{p(i)i})(t'_{ip(i)}h_{p(i)}t'_{p(i)i}) \mid 1 \leq i \leq n\}$.

Consider the product $t_{ki}t_{ik}$ for $1 \leq i, k \leq m$. We have $t_{ki}t_{ik} = \ell_k r_i \ell_i r_k = \ell_k x_1 r_k = \ell_k r_k = x_k$. Thus $t'_{p(i)i}t'_{ip(i)} = t_{a[p(i)]a(i)}t_{a(i)a[p(i)]} = x_{a[p(i)]} = y_{p(i)}$.

Hence $[\phi(p)(g)][\phi(p)(h)]$

$= \{t'_{ip(i)}g_{p(i)}y_{p(i)}h_{p(i)}t'_{p(i)i} \mid 1 \leq i \leq n\}$

$= \{t'_{ip(i)}g_{p(i)}h_{p(i)}t'_{p(i)i} \mid 1 \leq i \leq n\}$,

since $y_{p(i)}$ is the identity in the group $H_{y_{p(i)}} \ni g_{p(i)}, h_{p(i)}$.

Thus $\phi(p)(gh) = [\phi(p)(g)][\phi(p)(h)]$ for all $g,h \in \prod_{i=1}^{n} H_{y_i}$, and $\phi(p)$ is an homomorphism for all $p \in P_n$.

Hence $\phi(p)$ is an endomorphism of $\prod_{i=1}^{n} H_{y_i}$, and taking multiplication to be $\phi(p)\phi(q)(g) = \phi(p)[\phi(q)(g)]$ for all $p,q \in P_n$ and $g \in \prod_{i=1}^{n} H_{y_i}$, we have $\phi(p) \in \mathrm{Endo}_L(\prod_{i=1}^{n} H_{y_i})$.

(c) Now suppose $p,q \in P_n$ and $g = (g_1,\ldots,g_n) \in \prod_{i=1}^{n} H_{y_i}$.

Then

$$\phi(p)\phi(q)(g) = \phi(p)\{t'_{iq(i)}g_{q(i)}t'_{q(i)i} \mid 1 \leq i \leq n\}$$

$$= \{t'_{jp(j)}(t'_{p(j)q[p(j)]}g_{q[p(j)]}t'_{q[p(j)]p(j)})t'_{p(j)j} \mid 1 \leq j \leq n\} .$$

Now

$$t'_{ij}t'_{jk} = \ell_{a(i)}r_{a(j)}\ell_{a(j)}r_{a(k)} = \ell_{a(i)}x_1r_{a(k)} = \ell_{a(i)}r_{a(k)} = t'_{ik},$$

for all $1 \leq i,j,k \leq n$.

Thus

$$\phi(p)\phi(q)(g) = \{t'_{jq[p(j)]}g_{q[p(j)]}t'_{q[p(j)]j} \mid 1 \leq j \leq n\} .$$

But for $p,q \in P_n$ we have $pq(i) = q[p(i)]$, for $1 \leq i \leq n$.

Thus $\phi(pq)(g) = \{t'_{jpq(j)}q_{pq(j)}t'_{pq(j)j} \mid 1 \leq j \leq n\}$

$= \phi(p)\phi(q)(g)$ for all $g \in \prod_{i=1}^{n} H_{y_i}$.

Hence ϕ is an homomorphism.

(iii) Recall the definition of the map $\psi : H_s \to (\prod_{i=1}^{n} H_{y_i}) \times P_n$ in part (i).

Suppose $g,h \in H_s$. (<u>Not</u> in $\prod_{i=1}^{n} H_{y_i}$).

Then $\psi(g)\psi(h) = (g_1,\ldots,g_n,P_g)(h_1,\ldots,h_n,P_h)$.

Setting $g = \{(q_i, y_{iP_g(i)}, q_{P_g(i)}) \mid 1 \leq i \leq n\}$, where

$y_{iP_g(i)} = g_i t'_{iP_g(i)}$, $1 \leq i \leq n$,

and $h = \{(q_i, z_{iP_h(i)}, q_{P_h(i)}) \mid 1 \leq i \leq n\}$, where

$z_{iP_h(i)} = h_i t'_{iP_h(i)}$, $1 \leq i \leq n$,

we find

$g.h = \{(q_i, y_{iP_g(i)}, q_{P_g(i)}).(q_{P_g(i)}, z_{P_g(i),P_h[P_g(i)]}, q_{P_h[P_g(i)]}) \mid 1 \leq i \leq n\}$,

from lemmas 5.5, 5.6 and 5.7.

Thus $g.h = \{(q_i, y_{iP_g(i)} z_{P_g(i)P_h[P_g(i)]}, q_{P_h[P_g(i)]}) \mid 1 \leq i \leq n\}$.

We see that $P_{g.h}(i) = P_h[P_g(i)]$ for $1 \leq i \leq n$, so that $P_{g.h} = P_g P_h$, when the multiplication is considered in P_n.

Now

$y_{iP_g(i)} z_{P_g(i)P_{g.h}(i)} = g_i t'_{iP_g(i)} h_{P_g(i)} t'_{P_g(i)P_{g.h}(i)} = (g.h)_i t'_{iP_{g.h}(i)}$,

since $g.h = \{(q_i, (g.h)_i t'_{iP_{g.h}(i)}, q_{P_{g.h}(i)}) \mid 1 \leq i \leq n\}$.

(We have $\psi(g.h) = [(g.h)_1, \ldots, (g.h)_n, P_{g.h}]$).

Hence

$(g.h)_i \ell_{a[i]} r_{a[P_{g.h}(i)]} = g_i \ell_{a(i)} r_{a[P_g(i)]} h_{P_g(i)} \ell_{a[P_g(i)]} r_{a[P_{g.h}(i)]}$.

Multiplying both sides of this equation on the right by $\ell_{a[P_{g.h}(i)]}$, and recalling that $r_j \ell_j = x_1$ and $\ell_j x_1 = \ell_j$ for $1 \leq j \leq m$, we see that

$$(g.h)_i \ell_{a[i]} = g_i \ell_{a[i]} r_{a[P_g(i)]} h_{P_g(i)} \ell_{a[P_g(i)]} .$$

Further $(g.h)_i \ell_{a[i]} r_{a[i]} = (g.h)_i x_{a[i]} = (g.h)_i y_i = (g.h)_i$, since $(g.h)_i \varepsilon H_{y_i}$.

Thus $(g.h)_i = g_i t'_{iP_g(i)} h_{P_g(i)} \ell_{a[P_g(i)]} r_{a[i]}$

$= g_i t'_{iP_g(i)} h_{P_g(i)} t'_{P_g(i)i}$.

Hence $\psi(g.h) = \{(g_i t'_{iP_g(i)} h_{P_g(i)} t'_{P_g(i)i} \mid 1 \leq i \leq n),\ P_g.P_h\}$

$= \{(g_1,\ldots,g_n)\phi(P_g)(h_1,\ldots,h_n),\ P_g.P_h\}$

$= \{(g_1,\ldots,g_n),P_g\}\{(h_1,\ldots,h_n),P_h\}$ in $(\prod_{i=1}^{n} H_{y_i}) \times_\phi P_n$.

$= \psi(g).\psi(h)$.

(iv) Thus ψ is an homomorphism from H_s into $(\prod_{i=1}^{n} H_{y_i}) \times_\phi P_n$, and as was shown in (i), ψ is 1:1.

Thus $H_s \mid (\prod_{i=1}^{n} H_{y_i}) \times_\phi P_n$. #

5.9 DEFINITION Let $w = (q,x,q)$, $w' = (q',x',q') \varepsilon T(M)$, such that $x^2 = x$, $(x')^2 = x'$ and $x,x' \varepsilon J$, where J is a $\mathcal{J}$ class of $S(M)$.

Define $DSww'(J) = \{(q,y,q') \varepsilon T(M) \mid y \varepsilon J$ and $x \mathcal{R} y \mathcal{L} x'\}$.

From earlier lemmas we see that $w.(q,y,q').w' = (q,y,q')$ when $y \varepsilon J$ iff $(q,y,q') \varepsilon DSww'(J)$.

Further, if $DSww'(J) \neq \emptyset$ and $DSw'w''(J) \neq \emptyset$, where $w'' = (q'',x'',q'')$ and $(x'')^2 = x''$, then $DSww''(J) \neq \emptyset$.

Also if $DSww'(J) \neq \emptyset$, then $DSw'w(J) \neq \emptyset$. For suppose $(q,y,q') \varepsilon DSww'(J)$ and $(q',y',q'') \varepsilon DSw'w''(J)$, where

$w'' = (q'',x,q'')$. Certainly there exists w'' of this type, such that $DSw'w''(J) \neq \emptyset$, for $R_{x'} \cap L_x \neq \emptyset$, so that there exists y' with $y' \mathcal{R} x'$, and $y' \mathcal{L} x$. Then $q'' = q'.y' \in Z(y')$. But $yy' \in H_x$, so that $Z(yy') = Z(x)$. Thus $(q'',x,q'') \in T(M)$, and $(q',y',q'') \in DSw'w''(J)$. Now $yy' \in H_x$, implies the existence of $(yy')^{-1}$ such that $(yy')\ (yy')^{-1} = x$. Suppose $q''.(yy')^{-1} = q_1$. Then $q.(yy')\ (yy')^{-1} = q_1$, i.e. $q.x = q_1$. But $(q,x,q) \in T(M)$ so that $q \in Z(x)$. Thus $q.x = q$. Hence $q_1 = q$, and $(q'',(yy^1)^{-1},q) \in DSw''w(J)$. Hence $DSw'w(J) \neq \emptyset$.

Thus the relation R_J on $\{(q,x,q) \in T(M) \mid x \in J \text{ and } x^2 = x\}$ defined by $w\ R_J\ w'$ iff $DSww'(J) \neq \emptyset$, is an equivalence relation.

<u>5.10 LEMMA</u> Let $s.s = s \in S(J)$. Let $s = L(s) = N(s) = \{w_1,\ldots,w_n\}$.

Let $s = \bigcup_{i=1}^{k} s_i$, where $\emptyset \neq s_i \subseteq s$ for $1 \leq i \leq k$, such that $\{w_j,w_\ell\} \subseteq s_i$ iff $DSw_jw_\ell(J) \neq \emptyset$ for $1 \leq \ell,j \leq n$ and $1 \leq i \leq k$.

Then $H_s \mid \prod_{i=1}^{k} H_{s_i}$.

<u>Proof</u> : From the definition we see that $s_i \cap s_j = \emptyset$ iff $i \neq j$, and that $(s_i)^2 = s_i$ for $1 \leq i \leq k$.

Let $g \in H_s$. Suppose $DSww'(g) \neq \emptyset$ for $w,w' \in N(s)$. Then there exists $(p,x,q) \in g$ such that $w.(p,x,q).w' = (p,x,q)$. Certainly $(p,x,q) \in T(M)$, and $(p,x,q) \in DSww'(J)$. Thus $w,w' \in s_i$ for some i such that $1 \leq i \leq k$. Also $g = N(s).g.N(s) = \bigcup_{w,w' \in N(s)} DSww'(g)$.

Now let $(p,x,q) \in s_i.g$. Then $(p,x,q) = w.(p,x,q).w'$ for $w \in s_i$ and $w' \in N(s)$. But it was shown above that $(p,x,q) \in g$

implies $w' \varepsilon s_i$. Thus $(p,x,q) \varepsilon g.s_i$. The converse is similarly shown. Thus $g.s_i = s_i.g$ for $1 \leq i \leq k$. Further we see from this proof that $s_i.g \subseteq s_i.g.s_i$. But $s_i.g.s_i \subseteq s_i.g$ $(g.s_i \subseteq g)$, so that $s_i.g = s_i.g.s_i = g.s_i$ for $1 \leq i \leq k$.

Put $g_i = s_i.g.s_i$ for $1 \leq i \leq k$.

Then $g = \bigcup_{i=1}^{k} g_i$, since $g = N(s).g = \bigcup_{i=1}^{k} s_i.g$. (*)

Let $g,h \varepsilon H_s$.

Then $g_i.h_i = s_i.g.h.s_i = s_i.(g.h).s_i = (g.h)_i$, for $1 \leq i \leq k$. (**)

It is then easily seen by substitution for g and h in the above equation that $g_i \varepsilon H_{s_i}$, for $1 \leq i \leq k$.

Consider the map $\psi : H_s \to \prod_{i=1}^{k} H_{s_i}$, defined by :

$$\psi : g \mapsto (g_1,\ldots,g_k), \quad \text{for all } g \varepsilon H_s.$$

The ψ is an homomorphism (**), and 1:1 (*).

Hence $H_s | \prod_{i=1}^{k} H_{s_i}$. #

<u>5.11 LEMMA</u> Let $s.s = s \varepsilon S(J)$. Let $s = L(s) = \{w_1,\ldots,w_n\}$ such that $DSw_iw_j(J) \neq \emptyset$ for all $w_i,w_j \varepsilon s$.

Then $P_n | H_s$, where $n = |s|$.

<u>Proof</u> : Let $p \varepsilon P_n$. Let $h \varepsilon S(M)$ such that

$h \varepsilon \bigcup_{i=1}^{n} DSw_iw_{p(i)}(J)$, and $|DSw_iw_{p(i)}(J) \cap h| = 1$ for $1 \leq i \leq n$.

It was shown in the proof of lemma 5.7 that such an element of $S(M)$ must also be an element of H_s in $S(J)$.

Certainly $P_h = p$, where P_h is as defined in (5.7).

[Nowhere in the proof referred to does the fact that $DSw_i w_{p(i)}(g)$ where $g \varepsilon S(J)$ is used rather than $DSw_i w_{p(i)}(J)$, affect the proof.]

Since $DSw_i w_j(J) \neq \emptyset$ for all $w_i, w_j \varepsilon s$ we must have $DSw_i w_{p(i)}(J) \neq \emptyset$, for $1 \leq i \leq n$. Thus there exists at least one $h \varepsilon H_s$ such that $P_h = p$.

Hence the map $\psi : H_s \to P_n$, defined by $\psi : g \to P_g$ for all $g \varepsilon H_s$, is onto. In (5.7) it was shown to be an homomorphism.

Thus $P_n | H_s$. #

<u>5.12 LEMMA</u> Let J be a $\mathcal{J}$ class of $S(M)$.

Then $\mathcal{S}(J) | \mathcal{S}(M)$.

<u>Proof</u> : Let $B(J) = \{\cup J' | J' \leq J$ where J' is a $\mathcal{J}$ class of $S(M)\}$.

Then $\mathcal{S}[B(J)]$ is a subsemigroup of $\mathcal{S}(M)$. For suppose $s,t \varepsilon \mathcal{S}[B(J)]$. Suppose $(p,x,q) \varepsilon s$, $(p',x',q') \varepsilon t$. Then $J_{x'} \leq J$ and $J_{xx'} \leq J_{x'}$ so that $J_{xx'} \leq J$ and $xx' \varepsilon B(J)$. Hence $st \varepsilon \mathcal{S}[B(J)]$ when the multiplication is in $S(M)$, for all $s,t \varepsilon \mathcal{S}[B(J)]$. Thus $st = s.t$ where the latter multiplication is in $\mathcal{S}[B(J)]$.

Now consider the mapping $\psi : \mathcal{S}[B(J)] \to \mathcal{S}(J)$ defined by :

$$\psi : g \mapsto \{(p,x,q) \ \varepsilon \ g | x \ \varepsilon \ J\} .$$

We have $\psi(g).\psi(h)$

$= \{(p,x,q).(p',x',q') | (p,x,q) \ \varepsilon \ \psi(g),\ (p',x',q') \ \varepsilon \ \psi(h)$ and $xx' \ \varepsilon \ J\}$.

$\subseteq \{(p,x,q)(p,x',q') | (p,x,q) \ \varepsilon \ g,\ (p',x',q') \ \varepsilon \ h$ and $xx' \ \varepsilon \ J\}$

$= \psi(g.h)$.

Further $(p,y,q) \in \psi(g.h)$ implies $(p,y,q) = (p,x,p')(p',x',q)$ where $(p,x,p') \in g$, $(p',x',q) \in h$ and $xx' = y \in J$. Thus $J_y \leq J_x$ and $J_y \leq J_{x'}$. But $x,x' \in B(J)$ so that $J_x \leq J_y$ and $J_{x'} \leq J_y$. Thux $x \; \mathcal{J} \; x' \; \mathcal{J} \; y$, and $(p,x,p') \in \psi(g)$, $(p',x',q) \in \psi(h)$. Hence $\psi(g.h) \subseteq \psi(g).\psi(h)$.

Thus ψ is an homomorphism.

Certainly ψ is onto, since each element of $\mathcal{S}(J)$ may be considered as an element of $\mathcal{S}[B(J)]$.

Thus

$$\mathcal{S}(J) \,|\, \mathcal{S}[B(J)] \subseteq \mathcal{S}(M).$$

and

$$\mathcal{S}(J) \,|\, \mathcal{S}(M). \qquad \#$$

5.13 DEFINITION Let $\mathcal{I}(J)$ be the set of idempotents of $\mathcal{S}(J)$ with the properties that if s is such an idempotent ;

$$s = L(s) = N(s).s.N(s),$$

and $\quad DSww'(J) \neq \emptyset$ for all $w,w' \in s$.

Define $n(J) = \max \{|s| \mid s \in \mathcal{I}(J)\}$.

Define $n(M) = \max \{n(J) \mid J$ is a $\mathcal{J}$ class of $S(M)\}$.

5.14 LEMMA Let J be a $\mathcal{J}$ class of $S(M)$.

Then if G is a group such that $G|Sch(J)$, then $G|P_{n(J)}$.

Proof : Let $y^2 = y \in J$. Then $H_y \cong Sch(J)$.

Let $A_1,\ldots,A_k$ be non-empty subsets of $Z(y)$ such that : $\{p,q\} \subseteq A_i$ for some i such that $1 \leq i \leq k$ iff there exists $(p,y',q) \in T(M)$ where $y' \in H_y$.

Now $Z(y') = Z(y)$ for all $y' \varepsilon H_y$, and $Z(y)|P(y')$ for all $y' \varepsilon H_y$. Thus the action of an element y' of H_y, on Q, is completely determined by its action on the set $Z(y) \subseteq Q$, that is by a permutation of $Z(y)$.

Further any element of H_y is completely determined by a set of permutations on the sets $A_1,\ldots,A_k$, since no element has the action of taking a state of one such set to a state of another.

We can determine a monomorphism therefore of H_y into $\prod_{i=1}^{k} P_{|A_i|}$. Hence $H_y | \prod_{i=1}^{k} P_{|A_i|}$.

Now $s_i = \{(p,y,p) | p \varepsilon A_i\}$ is an idempotent of $S(J)$, and is in fact an element of $I(J)$, for $1 \leq i \leq k$.

Certainly $|s_i| \leq n(J)$ and $|s_i| = |A_i|$, thus $P_{|A_i|} \mid P_{n(J)}$. Thus $G|P_{|A_i|}$ for any group G implies $G|P_{n(J)}$.

Thus $G|Sch(J) \cong H_y$ implies $G|P_{|A_i|}$ for $1 \leq i \leq k$, which implies $G|P_{n(J)}$.

Hence $G|Sch(J)$ implies $G|P_{n(J)}$. #

5.15 DEFINITION Following Krohn, Rhodes, Tilson [ARBIB], define the following :

(i) PRIMES is the set of all nontrivial simple groups.

(ii) Let S be a semigroup, then PRIMES $(S) = \{G \varepsilon \text{ PRIMES} : G|S\}$

(iii) Let T be a collection of semigroups,

PRIMES $(T) = \{\text{PRIMES } (S) : S \varepsilon T\}$.

5.16 MAIN THEOREM PRIMES $[S(M)]$ = PRIMES $[P_{n(M)}]$.

Proof :

Put $\mathcal{T} = \{\mathcal{S}(J) \mid J$ is a $\mathcal{J}$ class of $\mathcal{S}(M)\}$

$\mathcal{I}_1(J) = \{s \in \mathcal{S}(J) \mid s.s = s \in N(s).s.N(s)$ and $L(s) = N(s)\}$

$\mathcal{I}_2(J) = \{s \in \mathcal{I}_1(J) \mid s = L(s)\}$

$\mathcal{I}_3(J) = \{s \in \mathcal{I}_2(J) \mid DSww'(J) \neq \emptyset$ for all $w,w' \in s\}$.

$\mathcal{G}_1(J) = \{H_s \mid s \in \mathcal{I}_1(J)\}$

$\mathcal{G}_2(J) = \{H_s \mid s \in \mathcal{I}_2(J)\}$

$\mathcal{G}_3(J) = \{H_s \mid s \in \mathcal{I}_3(J)\}$

Then (i) PRIMES $[\mathcal{S}(M)]$ = PRIMES $(\mathcal{T})$ (3.21) & (5.12)

(ii) PRIMES $[\mathcal{S}(J)]$ = PRIMES $[\mathcal{G}_1(J)]$ for each $\mathcal{J}$ class, J, of S(M). from (4.36) and $H_s \mid \mathcal{S}(J)$ for all $s \in \mathcal{S}(J)$.

(iii) PRIMES $[\mathcal{G}_1(J)]$ = PRIMES $[\mathcal{G}_2(J)]$. (5.7) and $\mathcal{I}_2(J) \subseteq \mathcal{I}_1(J)$.

(iv) PRIMES $[\mathcal{G}_2(J)]$ = PRIMES $[\mathcal{G}_3(J)]$ (5.10) and $\mathcal{I}_3(J) \subseteq \mathcal{I}_2(J)$.

(v) PRIMES $[\mathcal{G}_3(J)] \subseteq$ PRIMES $\{Sch(J), P_{n(J)}\}$ (5.8)

(vi) PRIMES $[Sch(J)] \subseteq$ PRIMES $[P_{n(J)}]$ (5.14)

(vii) PRIMES $[\mathcal{G}_3(J)]$ = PRIMES $[P_{n(J)}]$ (5.11) and (v) & (vi)

Thus PRIMES $[\mathcal{S}(M)]$ = PRIMES $\{P_{n(J)} \mid J$ is a $\mathcal{J}$ class of S(M)$\}$.

Now $P_{n(J)} \mid P_{n(M)}$ for all $\mathcal{J}$ classes of S(M), and $P_{n(J)} = P_{n(M)}$ for at least one $\mathcal{J}$ class of S(M).

Hence PRIMES $[\mathcal{S}(M)]$ = PRIMES $[P_{n(M)}]$. #

5.17 REMARK The value of n(M) is an invariant of a given automaton $M = (Q,I,\lambda)$ and may be found by determining the value of n(J) for each $\mathcal{J}$ class of S(M).

As was shown before, we need to consider subsets of the set $Id(J)=\{(q,x,q) \in T(M) | x^2 = x \in J, q \in Q\}$, and find whether the subsets are in $I_3(J)$. The cardinality of the largest of these subsets is then $n(J)$.

Assume that we know the idempotents of J, and the action of each element of the group associated with each idempotent. (The idempotents may be found by constructing a representation of J^0 as a Rees matrix semigroup, as can the elements of their respective groups.)

Suppose $s \in Id(J)$. Then $s \in I_3(J)$ iff (i) $w.w' = \emptyset$ for all $w,w' \in s$ and (ii) $DSww'(J) \neq \emptyset$ for all $w,w' \in s$.

To check on condition (i), suppose $w = (q,x,q)$, $w' = (q',x',q') \in Id(J)$. Then $w.w' = \emptyset$ iff $q \neq q'$ or $Z(x) \not| P(x')$. ($Z(x) \not| P(x')$ iff $xx' \notin J$.)

For condition (ii), let $H = R_x \cap L_{x'}$. Then H is an H class of J. Let $y \in H$, and suppose $q.y = p$. Then if there exists $x_1 \in H_{x'}$ such that $p.x_1 = q'$, then $(q,yx_1,q') \in DSww'(J)$. [Since we assumed that we know the action on Q of all elements of $H_{x'}$ we can determine this existence.] If $DSww'(J) \neq \emptyset$, then $DSw'w(J) \neq \emptyset$ and $DSw'w''(J) \neq \emptyset$ where $w'' = (p,x',p)$. Certainly $p.x' = p$ since $Z(y) = Z(x')$. Thus $DSw''w'(J) \neq \emptyset$, that is there exists $x_2 \in H_{x'}$ such that $(p,x_2,q') \in T(M)$. Thus (ii) is equivalent to: there exists $z \in H_{x'}$ such that $p.z = q$ where $q.y = p$ for any $y \in R_x \cap L_{x'}$.

These procedures could be programmed for computer solution of the problem of finding $n(J)$, and hence $n(M)$.

BIBLIOGRAPHY

ARBIB, M.A. Algebraic Theory of Machines, Languages and Semigroups.
Academic Press, New York & London, 1968.

CLIFFORD, A.H. & PRESTON, G.B.
The Algebraic Theory of Semigroups. Vol. I.
American Mathematical Society, Rhode Island, 1961.

FLECK, A.C., HEDETNIEMI, S.T.
S-Semigroups of Automata.
Technical Report No.6, THEMIS project, AD684842,
University of Iowa, IOWA.

FLECK, A.C., HEDETNIEMI, S.T., and OEHMKE, R.H.
S-Semigroups of Automata.
Journal of the Association for Computing
Machinery, 19, 3-10 (1972).

GREEN, J.A. On the Structure of Semigroups.
Annals of Mathematics, 54, 163-172 (1951).

KROHN, K. & RHODES, J.L.
Algebraic Theory of Machines. I. Prime Decomposition
Theorem for Finite Semigroups and Machines,
Trans.Amer.Math.Soc. 116, 450-464 (1965).

REES, D. On Semigroups.
Proc. Cambridge Phil.Soc. 36, 387-400 (1940).